TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ 2,00 €
SOLO INFORMAZIONE E ARTICOLI

n. 160
www.hackerjournal.it



LINUX DAY



INTERVISTA agli organizzatori

BLINDA il tuo Pinguino

DRM
Se li CONOSCI li EVITI

CHROME
Prime impressioni sul BROWSER di Google

DIFENDIAMO IL TORRENT
COME FUNZIONA e COME USARLO al meglio

QUATTORD. ANNO 8 - N°160 - 25 SETTEMBRE/8 OTTOBRE 2008 - € 2,00



Anno 8 – N.160
25 settembre/ 8 ottobre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



I nuovi **schiavi**

"La libertà è la misura della maturità di un uomo e di una nazione."
Giovanni Paolo II (Karol Wojtyla) (1920-2005)

Siamo tutti impressionati dalle immagini dei bambini nelle miniere di diamanti africane, da quelle dei lavoratori cinesi segregati nelle case italiane a lavorare per venti ore al giorno, dalle notizie di piccoli lavoratori assoldati dalle multinazionali della moda, in forma diretta o indiretta, per cucire scarpe, palloni e altro.

Siamo tutti impressionati e ci riteniamo fortunati e onorati di essere parte di un mercato, quello dell'informatica, dove lo sfruttamento di queste forma di lavoro non esiste, o meglio, non esisteva...

Tutti noi ci siamo imbattuti in un captcha, io personalmente li odio, e sappiamo tutti che vengono utilizzati per evitare che macchine possano effettuare registrazioni multiple automatizzate, per esempio a sistemi di mail o a Facebook, per poi inviare virus o altro. Il sistema funziona bene, difatti le macchine non riescono a scavalcare questo sistema, ma caratteristica dell'uomo è quella di, citando Eastwood/Gunny, "improvvisare, adattarsi e raggiungere lo scopo" soprattutto quando ci sono di mezzo soldi e affari sporchi e così eccoci con una nuova generazione e specie di schiavi: i compilatori di captcha...

Eserciti di disperati, soprattutto nei paesi orientali tipo India e Pakistan vengono assoldati per pochi dollari e impegnati a scrivere chiavi d'accesso tutto il giorno e, sebbene siamo tutti d'accordo sul fatto che sia meglio che spaccare pietre, si tratta comunque di schiavismo e non possiamo che esserne indignati.

Il nostro mondo non è più così lindo e sterile, rendiamocene conto!!!

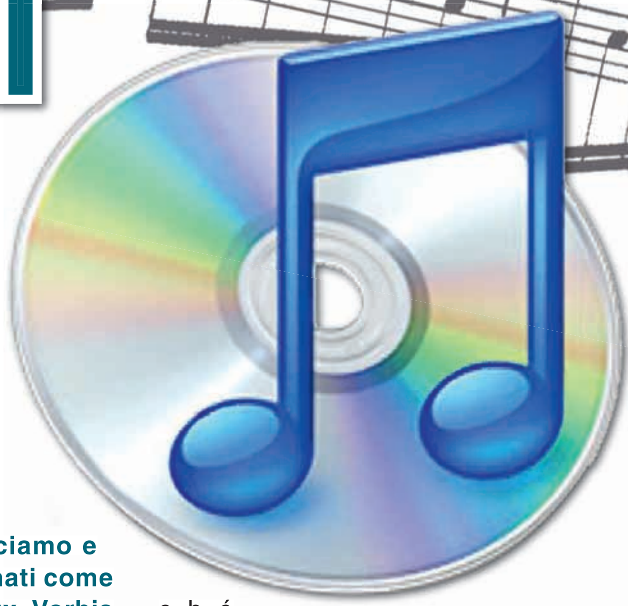
BigG

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

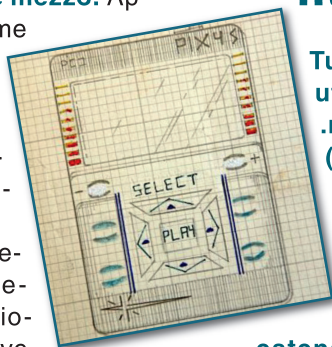
redazione@hackerjournal.it

iPod e dintorni

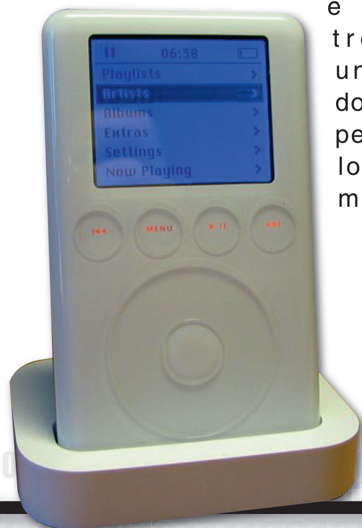


:: Il nonno dell'iPod salva Apple

Correva l'anno 1979 quando un simaptico inventore inglese di nome Kane Kramer depositò all'ufficio brevetti il suo progetto denominato IXI, una sorta di scatoletta di plastica in grado di riprodurre musica per tre minuti e mezzo. Apple ama quest'uomo come forse non ha mai amato nessuno e il motivo è semplice da intuire se si pensa a cosa sta succedendo tra l'azienda di Cupertino e la Burts.com. Quest'ultima ha citato Steve Jobs e soci per ottenere i diritti sull'invenzione dell'iPod come già aveva fatto con Microsoft e, proprio come con Bill Gates, è riuscita a spuntare un accordo economico per 10.000.000 di dollari a titolo di royalty.



Ora, l'accordo non è ancora firmato e Apple tira fuori dal cilindro una persona con un brevetto simile a quello impugnato da Burts.com ma precedente e che quindi lo annulla. Inoltre il sig. Kramer non naviga nell'oro e sta ora trovando un accordo con Cupertino per lo sfruttamento del suo brevetto, accordo che siamo certi non sarà così oneroso come quello con Burts.com.



:: Windows si dimentica di iTunes

Tutti noi conosciamo e utilizziamo formati come .mp4, .xvid, .divx, Vorbis (.ogg) e .m4v, allora viene spontaneo chiedersi come mai alla MIcrosoft nessuno piazza un tecnico ad aggiornare i database delle estensioni accettate. Quello che sembra particolarmente strano è che tra questi formati sia compreso proprio quello dei file con DRM scaricati da iTunes Store, con questo non vogliamo dire che Microsoft cerchi di boicottare lo shop on-line, anche perché sarebbe quasi impossibile, ma certo rende la vita più complessa ai suoi utenti. Un'altra considerazione riguarda la diffusione di questi formati, analizzando quanto riconosciuto e quanto no da Windows risulta chiaro che siano sicuramente di più le fonti non riconosciute che, per esempio, quelle con formati nativi di Redmont...
Speriamo che Ballmer e soci si decidano ad investire la folle cifra di un paio di centoni per il tecnico... ■





SPORE GIÀ CRACCATO

Le creature bizzarre di Spore, il nuovo videogame di Will Wright, hanno cominciato a popolare la rete BitTorrent con i download del gioco. Un download che, come spesso accade in questi casi, non è legittimato dai detentori del copyright, nella fattispecie la software house Maxis e il publisher Electronic Arts. Definito il primo "massively single-player online game", Spore è il lascito del designer che ha creato SimCity e i suoi tanti emuli e The Sims, che si è infine convertito ai "god game" lasciando da parte le piccole faccende quotidiane di agglomerati cittadini e teenager alla moda per lavorare su una prospettiva più universale.

EXPLORER 8 BLOCCA TUTTO

Quando si parla di sicurezza nella navigabilità in casa Microsoft non si scherza per niente. Infatti hanno annunciato, nell'ultimo comunicato stampa, che con l'uscita della seconda beta di Internet Explorer 8 saranno introdotti nuovi sistemi di protezione della privacy chimate InPrivate.

Il nuovo browser prevede il blocco di finestre pop-up, la possbilità di non far memomirizzare al computer la cronologia dei siti visitati, dei cookie o dei dati inseriti dei form. L'utente sarà avvisato dei tentativi di tracciamento della propria navigazione da parte di siti maligni i quali verranno messi in "quarantena" in una sotto directory per poi essere rivalutati sulla navigabilità dall'utente.



La cosa che fa preoccupare di più il mondo dellla pubblicità online, invece, è che Explorer 8 fermerà autonomamente tutti i banner pubblicitari e tuttu i messaggi intrusivi non lasciando visibilità a chi paga per avere spazio pubblicitario sul web.

SERVER LINUX BUCATI

I Cert americano, in questi giorni, ha dichiarato che pericolosi e maligni cracker starebbero sondando la maggior parte dei sistemi Unix statunitensi con una accurata dedizione per quelli installati su server aziendali. Molte le agenzie di software sono già state attaccate o bucate dai malfattori e richiedono un'azione riparatoria da parte dei creatori del pinguino informatico.



La porta d'entrata usata da questi ignoti è OpenSsh che non è ancora stato aggiornato dalla sua casa madre e quindi rimane soggetto a molte vulnerabilità. Il rootkit che infetta le macchine si chiamerebbe phanlanx2 e per identificarlo basterebbe lanciare il comando cd il quale lo rileverebbe nella directory nascosta /etc/khubd.p2/.

RED HAT INVIOLABILE

Settimana scorsa la famosa software house Red Hat è stata attaccata da ignoti malfattori che hanno provato ad entrare nei pacchetti OpenSsh dei server Enterprise Linux 4 e 5. Ma in casa Red Hat i danni sono irrisori o limitati a qualche sotto cartella. La casa produttrice ha retto molto bene il colpo e non ha permesso a questi pirati informatici di introdursi nei sistemi per sostituire le signature dei pacchetti



HOT NEWS

BEST WESTERN L'HOTEL VIOLATO!

"L'ingresso è avvenuto attraverso il terminale di un hotel che non può in nessun caso, perché non è collegato direttamente, colloquiare con il CRS centrale dove sono contenuti i dati dei clienti. L'applicazione degli alberghi infatti è abilitata al dialogo on line per quanto riguarda tariffe e prezzi, statistiche ma non per i dati dei clienti". Best Western ribadisce inoltre che "l'ID utente violato è riuscito ad accedere alle prenotazioni di un singolo hotel e non c'è traccia di accesso non autorizzato ai dati di altri hotel Best Western. Il sistema Best Western non conserva i dati di prenotazione oltre la data di partenza del cliente, limitando quindi la potenziale esposizione dei dati ai clienti di quello specifico albergo che (1) sono partiti entro quella data, (2) che stanno soggiornando e (3) che hanno prenotazioni con data di arrivo futura. Non c'è traccia di accesso non autorizzato ai dati di altri clienti". Comunicato stampa Best Western.



IL VAIO CHE SURRISCALDA

La Sony sta richiamando a casa più di 440.000 Vaio per problemi di surriscaldamento. Il problema starebbe nel cablaggio dei cavi interni che porterebbe questi modelli giapponesi a surriscaldarsi fino a deformare e persino fondefre la plastica esterna mettendo a rischio anche gli stessi utenti. I portatili interessati da questo difetto sono quelli con il numero di serie VGN-TZ100, VGN-TZ200, VGN-TZ300 e VGN-TZ2000. Sony invita i proprietari di questi esemplari a visitare la pagina web di supporto dell'azienda e verificare l'eventuale appartenenza a questa "Bad List". Le unità in questione sono state prodotte tra luglio 2007 e agosto 2008 e nella maggior parte dei casi riscontrati sono stati venduti in Giappone.



XBOX COSTA MENO

Dopo aver visto il grande successo della concorrente Nintendo Wii, i collaboratori di Redmond in Microsoft hanno pensato di abbassare notevolmente il costo di tutte le versioni della Xbox 360. Infatti il prezzo della versione base costerà meno della concorrente Wii di 50 dollari. Dall'11 settembre la Xbox 360 Arcade costerà 199 dollari invece che 279, la Pro da 60 GB 299 dollari e la versione Elite da 120 GB a 399.
Questo rilancio, dicono in Microsoft, dovrebbe far recuperare terreno sulle concorrenti soprattutto durante le vendite natalizie.



operativi. Se ci fossero riusciti, i malintenzionati, avrebbero potuto diffondere in tutta la rete software modificati e comandati che avrebbero permesso poi l'attacco ai server che richiedevano i diversi aggiornamenti forniti dalla Red Hat. E non sarebbe stato danno da poco visto che i loro software sono utilizzati in aeroporti, banche, distribuzioni internazionali e molti altri servizi sensibili.



Poker online anche in Italia

Si era già visto sui nostri schermi ma non tutti sapevano che il poker online stava facendo solo un giro di rodaggio. Ora i Monopoli di Stato hanno dato l'effetivo nulla osta alle giocate via internet ed è già polemica. Gioco Digitale sarà il primo sito autorizzato per le video giocate che aprirà le sue porte non appena finirà i test sui sistemi di sicurezza. Si potrà puntare da un minimo di 50 centesimi ad un massimo di 80 euro. I premi, invece, verranno così distribuiti: l'80% al vincitore, il 3% allo stato e il restante 17% al gestore del gioco. Le previsioni vedono un aspettativa di 200.000 persone nella prima settimana e 500.000 nella seconda per un affare di soldi da capogiro.



NUOVA PSP-3000

Sony ha annunciato la nuova uscita per la PlayStation Portable 3000 che arriverà sui nostri mercati l'anno prossimo. La nuova console portatile si potrà collegare via internet e prevederà un microfono integrato per parlare con gli altri giocatori o telefonare tramite Skype.
Il monitor Lcd da 4,3 pollice avrà una maggiore luminosità e fluidità di immagine che però farà calare di 20-30 minuti l'autonomia del nuova PSP proprio per le maggiori richieste di energia richieste dal monitor. I prezzi oscillano dalle 125 euro per il Giappone e 199 euro per l'Europa.

ARRIVANO I NUOVI IPOD



Proprio in questi giorni a San Francisco vengono presentate le nuove versioni dell'iPod di Apple. L'appuntamento è per martedi 9 settembre all'evento nominato "Let's Rock" dove verrano spiegate le nuove funzionalità, i design e i modelli oltre a qualche altra novità di Machintosh come l'ottava versione di iTunes.
In casa Apple hanno lasciato anche i più curiosi giornalisti a bocca asciutta sul trapelamento di news sui nuovi modelli ma fonti non ufficiali dicono che i nuovi iPod ritorneranno in una nuova veste arrotondata richiamando molto i modelli della prima e seconda serie.

TIM ATTACCATA

Il 2 settembre un attacco pirata ha messo in ginocchio i server Tim causando il blackout dei servizi di ricarica fatti dal 4916, numero gratuito della compagnia che permette di ricaricare il credito della propria scheda Tim. Infatti il virus non permetteva l'erogazione del credito sui telefonini mettendo i clienti in subbuglio che hanno fatto collassare il servizio clienti Tim con richieste di risarcimento per la non ricarica del credito prepagato. I servizi erano comunque disponibili da qualsiasi punto Sisal, Lottomatica o Bancomat. Secondo gli operatori il problema sarebbe stato risolto nell'ambito delle 24 ore, ma in realtà il blackout rimase anche nei due giorni seguenti con risoluzioni a singhiozzo per i clienti.



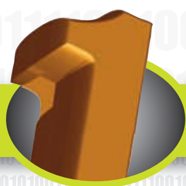
VIVIANE REDING SANTA SUBITO

Il Commissario Europeo alle Comunicazioni Viviane Reding dichiara guerra ai costi degli sms e della navigazione in rete. Infatti, in Parlamento Europeo, è stata presentata una mozione sulla quale tutti i paesi europei dovranno votare che porterà al drastico abbassamento dei costi che si ha mandando un sms da un paese dell'Unione Europea ad un altro. Basta pensare che oggi paghiamo dai 30 agli 80 centesimi a messaggio per un a media di 2,5 sms al giorno per paese. La Reding vorrebbe portare questa soglia almeno a 11 centesimi e portare il prezzo di un Mb, scaricato da cellulare, a 1 euro più tosto che 3 o 4.



500 MILIONI DI SPAM

Chi non ha dovuto almeno una volta nella vita cambiare casella di posta elettronica perché invasa troppe volte dallo spam? Invece no, non è così. Lo spam non è indirizzato a tutti noi ma solo ai più sfortunati che hanno come iniziale della mail le lettere A, M, S, R o P.
Richard Clayton, noto ricercatore dell'università di Cambridge, ha dimostrato che con queste particolari




DELL INSPIRON 910

Ha debuttato lo scorso 4 settembre il nuovissimo "mini" portatile della Dell chiamato Inspiron 910. L'ultimo prodotto della Dell dovrebbe fare una concorrenza spietata all'acerrimo nemico Eee Pc di Asus. Il "piccolino" della Dell monta un processore a singolo core Intel Atom N270 da 1,6 GHz, accompagnato da 512 Mbyte oppure 1 Gbye di ram Ddr2. Il display misura 8,9 pollici in diagonale e ha una risoluzione di 1024x600 pixel, mentre per il disco rigido si parla di unità Ssd da 4, 8 o 16 Gbyte. Come sistema operativo si può scegliere tra Windows Xp e Ubuntu Linux 8.04, mentre il prezzo è di 400 dollari. Tre porte Usb 2.0, supporto Wlan e Wwan, lettore di schede, porta Ethernet 10/100 e supporto Bluetooth via minicard completano la dotazione insieme alla batteria (da 2,2 o 2,6 Ah) per un peso complessivo inferiore al chilogrammo.



GTA IV SCANDALO IN THAILANDIA

La commisione per la tutela dei minori in Thailandia ha deciso che la serie GTA è classificata oscena e di conseguenza fuori legge. Tutto questo è stato deciso oggi dopo che il giovane Polwat Chinno, arrabbiato con i suoi genitori perché non lo facevano più giocare a GTA IV, era uscito di casa con un coltello da cucina e aveva accoltellando mortalmente un taxista rubandogli poi l'autovettura di servizio. Il giovane criminale era stato poi fermato qualche ora dopo dalla polizia e messo immediatamente in arresto. Polwat dichiarò che fece queste azioni perché non potendo giocare virtualmente a GTA IV l'aveva portato in real life provando la vera difficoltà di rubare un taxi come spesso bisogna fare nel video game. Ora il giovane Chinno rischia la pena di morte.



NOKIA MUSICA GRATIS

Anche Warner Music Group si è unito a Universal, Sony Bmg e Nokia per dare il via al progetto Comes with music, l'iniziativa che unisce l'acquisto di un telefono alla possibilità di scaricare legalmente brani musicali per un anno annunciata dall'azienda finlandese nello scorso aprile.
Il mercato che avrà l'onore di fare da apripista è quello inglese: da ottobre nel Regno Unito sarà in vendita per 70 sterline (circa 100 euro) il Nokia 5310, distribuito in esclusiva dall'operatore Carphone che già ha aperto le prevendite online.
Chi dunque acquisterà il Nokia 5310 Xpress Music avrà libero accesso per un anno ai cataloghi di Sony Bmg, Universal e Warner, dai quali potrà scaricare tutti i brani che vorrà; qualora poi desiderasse masterizzarli su Cd dovrà pagare una quota aggiuntiva non specificata.

iniziali la percentuale di spam nella propria casella di posta elettronica è del 40%, se invece le iniziali della propria mail deovessero essere la Q, Z o Y la percentuale si abbasserebbe drasticamente al 15%.
Questo particolare è dato dal fatto che le prime iniziali sono molto più popolari nei nomi rispetto ad altre e un attacco basato su dizionario ricerca proprio i nomi comuni di cose o persone che quindi le predilige. Lo studio di Clayton è stato basato su 500 milioni di mail spazzatura.

QUASI FANTASCIENZA

I ricercatori del Boston College sono riusciti a produrre una sorta di nanoragnatela flessibile con l'obiettivo di impiegarla in campo elettronico e nel settore della produzione energetica. Il team, guidato da Dunwei Wang descrive il risultato dello studio come una ragnatela bidimensionale composta da nanofili. Costituiti da titanio e silicio, questi nanofili si intrecciano in una struttura regolare, piatta. Pur essendo estremamente sottili, queste nanoreti mantengono intatta la loro complessità strutturale e si sono dimostrate in grado di trasportare una carica elettrica. La crescita, infatti, è molto lenta in entrambe le direzioni: secondo i ricercatori, le nanoreti crescono spontaneamente dal basso verso l'alto mediante semplici reazioni chimiche, provocate da una sostanza attivatrice. La sfida che Wang vorrebbe fronteggiare è la cosiddetta sfida dei terawatt, per vincere la quale "occorre impiegare materiali abbondanti ed economici".

Linux Day 2008

Abbiamo scambiato quattro chiacchiere con uno degli organizzatori della giornata del pinguino, eccovi cosa ci siamo detti

Giunto alla 8° edizione il Linux Day si è ormai consolidato come uno degli appuntamenti più importanti per gli amanti del Pinguino e del software libero in generale. Ne abbiamo parlato con Michele Dalla Silvestra membro dell'Italian Linux Society.

1. Ciao Michele e grazie per aver accettato la nostra intervista. Per prima cosa, vi chiedo di presentarvi. Cosa é ILS (Italian Linux Society)?

La Italian Linux Society nasce nel lontano 1994, agli albori della connessione alla rete Internet di massa in Italia, di pari passo con il diffondersi del sistema operativo Gnu/Linux.

Il nostro scopo é promuovere e sostenere iniziative per la diffusione del sistema operativo Gnu/Linux in Italia, e delle soluzioni informatiche basate sul software libero.

Entrando nel dettaglio il nostro obiettivo é favorire la libera circolazione delle idee e della conoscenza in campo informatico, promuovere lo studio ed il libero utilizzo delle idee e degli algoritmi che sottendono al funzionamento dei sistemi informatici, promuovere l'applicazione del metodo sperimentale nello studio dei sistemi informatici.

Per realizzare i nostri obiettivi, la ILS sviluppa studi e ricerche nel settore dell'informatica, organizza convegni, manifestazioni e corsi per la divulgazione della cultura informatica.

La ILS organizza con cadenza annuale la nota manifestazione Linux Day, una intera giornata dedicata al sistema operativo Gnu/Linux e al software libero, realizzata in contemporanea in molte città d'Italia. La prima edizione si é svolta nell'anno 2001.

2. Linux day é giunto ormai alla sua ottava edizione: esiste il rischio di ripetersi?

La natura del Linux Day é stata, da sempre, divulgativa. Molte persone si sono avvicinate al mondo del software libero e hanno adottato il sistema operativo Gnu/Linux in seguito ad una prima partecipazione alla manifestazione.

Le persone che ancora ignorano l'esistenza di personal computer che funzionano grazie ad un sistema operativo ed un pacchetto di office automation diversi da quelli proprietari, sono purtroppo ancora la maggioranza.

D'altra parte il software libero é entrato a far parte del corredo di pacchetti all'interno delle imprese, della pubblica amministrazione e di molti privati, nonché oggetto di ricerca nelle università.

Gli argomenti sono tanto vasti e variegati, e il pubblico così eterogeneo che no, non pensiamo il rischio di ripetersi esista.



3. Il software libero, rispetto al 2001, ha visto crescere la sua diffusione ed é diventato una realtà consolidata nelle imprese e nella pubblica amministrazione, quanto é maturo il mercato del software libero in Italia?

Difficile rispondere a questa domanda. Le piattaforme basate sul software libero sono abbastanza diffuse in ambito server, grazie agli alti standard di affidabilità e sicurezza.

Dal lato desktop aziendale e privato, lo strapotere della soluzione proprietaria più nota é palese.

Il software libero rappresenta comunque una seria alternativa e opportunità di costruire sistemi informativi affidabili e integrati con il mondo proprietario.

Il mercato del software libero al momento é immaturo in Italia, a causa di limiti di know how delle aziende che fanno domanda e delle imprese che realizzano l'offerta.

Ma il mercato di soluzioni basate esclusivamente o in parte sul software libero é in costante crescita.

4. Perchè secondo voi Linux non viene usato dalla maggioranza degli utenti?

Il motivo storico é il supporto hardware da parte dei produttori, inesistente o in rari casi inadeguato alle aspettative dell'utente, sopratutto l'utente meno smaliziato.

5. Cosa bisognerebbe fare affinché Linux e il software libero possano avere maggiore "appeal" tra i giovani?

Come abbiamo risposto alla precedente domanda, il sistema operativo Linux é scarsamente supportato dai produttori di hardware. Le applicazioni pesantemente multimediali e di videogioco ne risentono e questo rende Linux meno appetibile per una larga fetta di pubblico giovane.
D'altro canto, la curiosità innata delle giovani menti, e il tempo libero a disposizione, portano i giovani a installare e usare Linux tramite il passa parola. Da questo punto di vista grande assente é la scuola che dovrebbe fare la sua parte, per la diffusione di un software utile e portatore di valori etici indiscutibili.

6. Usi la tua carica associativa per fare colpo sulle donne?
Prima faccio colpo, poi la uso. Ma è successo una sola volta...

7. Usi mai Windows? Se sì, l'hai regolarmente comprato o...?
Lo uso di rado o quando costretto, da clienti (dove la licenza è un problema loro) o sul pc portatile in cui la licenza mi è stata appioppata senza chiederlo e senza volerlo.

8. Quante ore passi davanti al computer?
7-8 ore al giorno.

9. E sotto il computer?
Ho un computer in mansarda, ci passo sotto varie volte durante la giornata ;-)

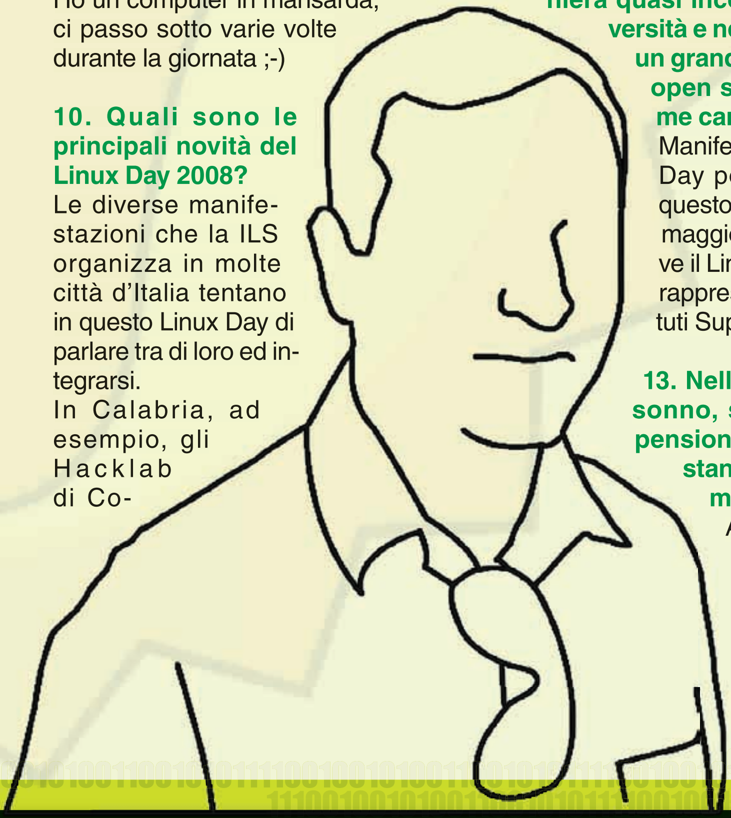
10. Quali sono le principali novità del Linux Day 2008?
Le diverse manifestazioni che la ILS organizza in molte città d'Italia tentano in questo Linux Day di parlare tra di loro ed integrarsi.
In Calabria, ad esempio, gli Hacklab di Cosenza, Catanzaro, Crotone, Vibo Valentia ed Altomonte, il RCLug di Reggio Calabria e il CSLug di Cosenza, organizzano una manifestazione denominata Linux Day Calabria con contenuti e integrazione dei temi a cura delle diverse associazioni, che parlano tra di loro per un obiettivo comune.
La ILS si impegna ad integrare sempre di più il Linux Day delle diverse città d'Italia al fine di farne una unica grande manifestazione, fruibile in ogni angolo della penisola, rispettando la individualità delle diverse associazioni aderenti all'iniziativa.

11. Quali sono, secondo voi, gli aspetti ancora carenti del Linux Day?
Una maggiore divulgazione da parte dei network di informazione nazionali, parlo di televisione generalista e grandi giornali in primo luogo.
Il software libero stenta a diventare oggetto di interesse da parte dei media e della opinione pubblica.
I temi scottanti della privacy e delle libertà digitali, al contrario sono molto sentiti grazie ai recenti fatti di cronaca, e potrebbero risvegliare l'interesse verso il software libero ed un uso consapevole della rete e del mezzo informatico.

12. Per quanto riguarda invece giovani e futuro, Microsoft e le piattaforme proprietarie dominano ancora in maniera quasi incontrastata nelle università e nei loro insegnamenti, un grande freno per il mondo open source. Perchè e come cambiare le cose?
Manifestazioni come il Linux Day possono fare molto in questo senso. Non a caso la maggior parte dei luoghi dove il Linux Day si svolge sono rappresentati da Scuole, Istituti Superiori e Università.

13. Nelle ore che dedichi al sonno, sogni più spesso il pensionato Bill Gates o l'instancabile Richard Stallman?
Almeno la notte sogno altra gente...

14. Il primo aggettivo che ti viene in mente per Bill Gates?
Furbo.



15. Per RichardStallman?
Idealista.

16. Qual è il tuo più grande sogno per il futuro dell'open source?
Che diventi il punto di riferimento principale quando si insegna l'informatica.

17. Se potessi realizzare un sogno, faresti un viaggio nello spazio come Mark Shuttleworth o ...
Potrebbe essere, ma non ci ho mai pensato. Fin'ora mi sono accontentato di volare a qualche centinaio di metri da terra.

18. Offrirai una birra a tutti i visitatori di Redomino Labs che< decideranno di partecipare al Linux Day dopo questa intervista?
Virtualmente si.

19. Qual è il tuo più grande sogno per il futuro dell'open source e del software libero?
Una umanità che usa in modo consapevole il mezzo informatico, la rete Internet e le nuove tecnologie. Non un consumo di massa, quindi, ma una grande coscienza collettiva che porterebbe idee e sviluppo sostenibile per il pianeta terra.

20. Dateci almeno tre buone ragioni per partecipare al Linux Day 2008 Conoscere la comunità del software libero, gente davvero simpatica e portatore di idee nuove e interessanti stili di vita.
Acquisire consapevolezza sull'uso del mezzo informatico, la privacy, i diritti digitali dell'individuo in rete.
Apprendere nuove tecnologie e sapere scientifico divulgato in modo ineccepibile al di fuori delle stanze delle università e dei centri di ricerca, come raramente accade nella nostra nazione.

21. L'intervista è conclusa, vuoi mandare un messaggio ai nostri lettori?
La rete é fatta innanzi tutto di persone, come dimostrato dal successo del social networking.
Andate al Linux Day con il sorriso sulle labbra e la mente aperta al sapere scientifico.

22. L'intervista è conclusa, vuoi mandare un messaggio ai nostri lettori?
Che il software libero sia con voi!

Sicurezza gratuita

Non c'è bisogno di aprire il portafoglio per difendere il PC dalle minacce informatiche. Possiamo infatti scaricare gratis tutto quel che ci serve: antivirus, firewall, antispyware...

Come va il nostro PC? Bene? Allora perché dovremmo continuare a leggere una rivista che tratta di sicurezza? Perché, lo sappiamo bene, al giorno d'oggi nessuno è davvero al riparo dal pericolo dei virus e di tutte le altre minacce informatiche! Ne esistono di ogni genere: spyware, malware, trojan, rootkit, adware... Chiunque purtroppo è destinato prima o poi a imbattersi in qualche malware. Meglio dunque non farsi cogliere impreparati e installare per tempo una "suite" di sicurezza. Se già lo abbiamo fatto, il pacchetto potrebbe però cominciare a sentire il peso degli anni o magari ce ne serve un altro che protegga un secondo computer, più vecchio, ma non abbiamo alcuna intenzione di sborsare soldi per una seconda licenza. Per fortuna, ci sono strumenti gratuiti che hanno la pretesa, talvolta giustificata, di rimpiazzare in tutte le loro funzioni suite commerciali come Norton 360, BitDefender Internet Security e Kaspersky Internet Security. Molte di queste applicazioni, peraltro, sono state sviluppate dagli stessi produttori di alcuni dei software che abbiamo appena citato.

Nel campo della sicurezza informatica, qualità può far rima con risparmio!





DIAGNOSTICA

PANDA SECURITY

Infected or Not?

PANDA SECURITY

Home

Utenti di

Utenti di

Utenti di

Utenti di altri antivirus



Il 22% di utenti con antivirus aggiornato è infetto*
...sei tra questi?

Non tutte le soluzioni antivirus sono uguali. Ora Panda Security riconosce **più di 3 milioni di minacce** grazie alla Collective Intelligence e possiamo offrire una protezione migliore.

Fare la spia non è proprio cosa da simpaticoni. Panda Security, tuttavia, sembra infischiarsene. Stando alle pagine di presentazione del servizio, infatti, il 22% degli utenti di un certo antivirus sarebbe infetto, nonostante l'aggiornamento tempestivo delle definizioni. Lo stesso vale per il 27% degli utilizzatori di un altro noto pacchetto e per il 17% di un terzo anonimo rivale. Di quali antivirus si parla? Nomi non se ne fanno, anche se i colori scelti per ciascuno di questi contendenti possono aiutarci nel riconoscerli. Questo genere di pubblicità comparativa può strappare qualche sorriso ma, per fortuna, ActiveScan fa decisamente sul serio. Una semplice scansione ci permetterà di rilevare minacce come virus, spyware e trojan. In caso di infezione ripuliremo il tutto con l'aiuto di un antivirus.

- **PRODUTTORE: PANDA**
- **WWW.INFECTEDORNOT.COM**

ANTIVIRUS

AVG FREE 8.0



Il motore di AVG Anti-Virus Free Edition non è altro che una versione alleggerita della versione commerciale I del programma: il nome del pacchetto resta identico, fatto salvo il "Free Edition", ovviamente. AVG Free non rileva i rootkit, non controlla i trasferimenti né la posta elettronica né le pagine Web visitate né tantomeno beneficia del servizio di assistenza allestito dal produttore. Ciò nonostante resta un eccellente antivirus capace di rilevare e sradicare anche i virus più ostinati, gli spyware e gli adware. In più offre una protezione contro l'utilizzo, a nostra insaputa, dei dati personali e controlla sistematicamente i risultati delle ricerche su Google, Yahoo! e Microsoft Live Search. Potremo evitare, così, di visitare siti dal contenuto potenzialmente nocivo, una vera chicca! L'unico difetto che presenta questo programma è dato dall'interfaccia disponibile solo in lingua inglese. Peccato, perché per il resto è davvero gradevole e, come nel caso di AntiVir, è anche piuttosto facile da regolare (pur permettendo agli utenti più esperti di accedere anche ai parametri di configurazione meno scontati). Per modificarli, eventualmente, basterà scorrere il menu Tool e selezionare la voce Advanced Settings. Tutto qui? Sì, ma come sottolinea lo stesso produttore potrebbe risentirne il livello generale di sicurezza. Insomma una soluzione semplice e miracolosa, allo stesso tempo, non c'è. Peccato perché ZoneAlarm, se ben configurato, è pressoché una "garanzia".

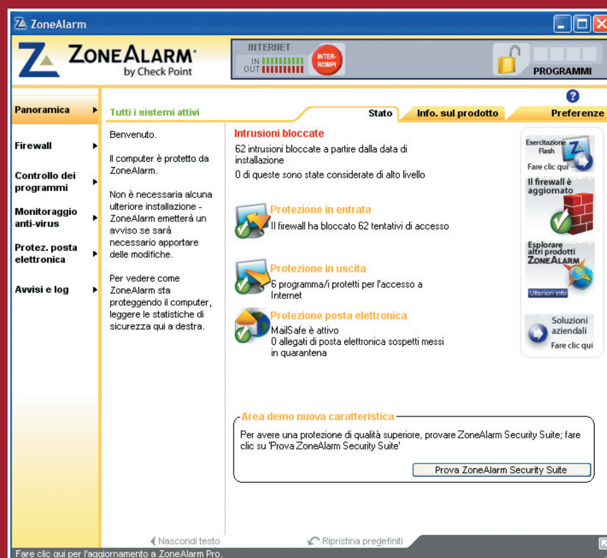
- **PRODUTTORE: CHECK POINT SOFTWARE TECHNOLOGIES**
- **WWW.ZONEALARM.COM**

FIREWALL

ZONEALARM 7.1

ZoneAlarm è disponibile gratuitamente per i privati e per le associazioni senza scopo di lucro. Si tratta di un firewall che ci protegge efficacemente da quei pirati e da quegli hacker che potrebbero infiltrarsi nel nostro computer mentre siamo connessi a Internet prendendone il controllo, compromettendone il buon funzionamento o, ancora, rubandoci dati sensibili o informazioni personali. In più si integra all'antivirus controllando, come prima cosa, che ce ne sia uno già installato, funzionante e aggiornato. Tutto questo in teoria, perché ci siamo sciaguratamente accorti che non riconosce certi antivirus, tra cui un pezzo da novanta come Norton Antivirus. Versione dopo versione l'interfaccia di ZoneAlarm è andata semplificandosi. Tuttora, tende a bombardarci di avvisi di ogni genere, cosa che potrebbe turbare gli utenti alle prime armi. "Questo programma richiede l'accesso a Internet...". Che fare? Nel momento in cui tutte queste notifiche diventassero noiose possiamo passare alla modalità automatica che ci permette di impostare una regola universale, scegliendo tra Autorizza o Rifiuta.

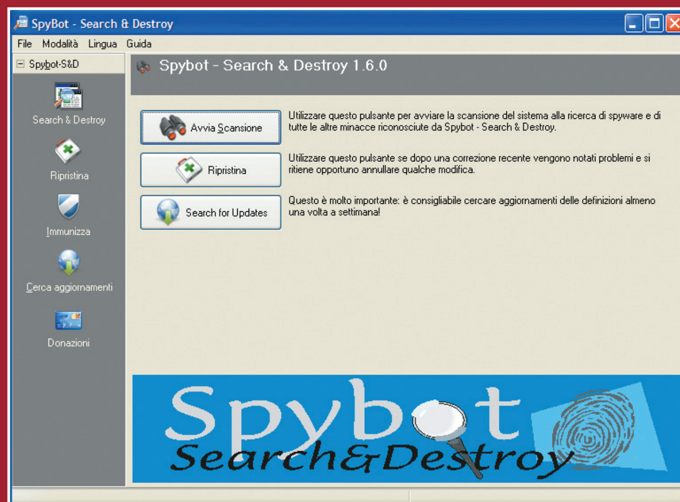
■ **PRODUTTORE: CHECK POINT SOFTWARE TECHNOLOGIES**
■ **WWW.ZONEALARM.COM**



ANTISPYWARE

SPYBOT SEARCH AND DESTROY 1.5.2

Spybot S&D ci permette di scovare e sradicare tutti gli spyware annidati nel nostro PC. Ciò include i trojan ma anche i cosiddetti keylogger, ossia piccoli programmi che registrano tutto quel che battiamo a tastiera, password incluse. A installazione avvenuta, un semplice clic su Search & Destroy ci garantirà una scansione esaustiva in cerca di eventuali minacce che saranno poi eliminate con efficacia. La modalità di funzionamento predefinita è piuttosto semplice. Attivando la Modalità Avanzata, invece, avremo più parametri da configurare: è riservata agli utenti più esperti. Il programma, prudentemente, ci propone, subito dopo l'installazione, di creare una copia di sicurezza del registro di Windows la quale ci permetterà di tornare alla configurazione originale del computer, nel caso qualcosa andasse storto. Spybot S&D crea, inoltre, un punto di ripristino dopo ogni sua correzione. Questi punti potranno essere recuperatii premendo il pulsante Ripristina che possiamo trovare sulla sinistra.





■ **PRODUTTORE: SAFER NETWORKING**
■ **WWW.SAFER-NETWORKING.ORG/IT**

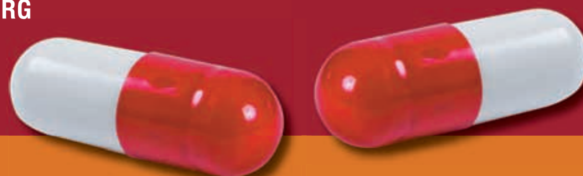
MALWARE

FILEASSASSIN 1.06



Purtroppo alcuni malware sono quasi irremovibili. Questo perché sono "ancorati" a file o programmi che Windows rifiuta ostinatamente di cancellare o di chiudere. Possiamo risolvere questo genere di guai con FileAssassin. Lanciamolo, scriviamo il nome del file che vorremmo cancellare poi selezioniamo Execute. File-Assassin, per cominciare, fermerà quei processi che tengono impegnato il file e poi lo cancellerà. Per i più esperti può funzionare anche tramite riga di comando, in modalità testo.

- PRODUTTORE: MALWAREBYTES
- WWWW.MALWAREBYTES.ORG



ANTITRUFFA

ROGUEREMOVER 1.24

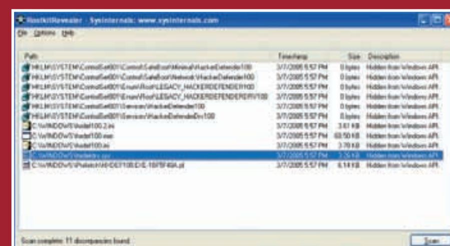


Quando si tratta di sicurezza talvolta rasentiamo la paranoia. Magari abbiamo anche la tendenza a scaricare ogni genere di applicazione contro gli spyware, i trojan, i rootkit e così via. Purtroppo non sempre è un'abitudine salutare. Ci sono svariati malware che si spacciano per strumenti contro gli uni e contro gli altri. Possiamo scovarli con un programma affidabile come RogueRemover. L'applicazione, disponibile in lingua italiana, è piuttosto semplice da usare. Installiamola e clicchiamo sul collegamento Scan: partirà una scansione che verificherà il contenuto dei dischi e del registro di Windows, in cerca di eventuali malware annidati sul nostro computer. Nel caso risultasse pulito il risultato dell'analisi sarà in verde. Nel caso contrario RogueRemover ci indicherà come sradicare i malware rilevati.

- PRODUTTORE: MALWAREBYTES
- WWW.MALWAREBYTES.ORG

ANTIROOTKIT

ROOTKITREVEALER 1.71



Come suggerisce il nome questa applicazione, targata Microsoft, è uno strumento per la rilevazione dei rookit, piccoli programmi che aprono porte TCP/IP sul nostro computer. Per beneficiarne appieno, però, occorre un po' di esperienza. Questo per evitare di cancellare, inavvertitamente, chiavi di registro o eseguibili che l'applicazione potrebbe scambiare per rootkit. La stessa Microsoft avvisa che Rootkit Revelear segnala le eventuali incoerenze nel registro di sistema in cerca di tracce che potrebbero indicare la presenza di un rootkit: si fa ampio ricorso al condizionale. Meglio salvare i risultati e sottoporli a un esperto. Il programma è solo in inglese. La funzione di ricerca del sito italiano di Microsoft non permette di rintracciarlo con precisione. Consigliamo di scaricarlo dall'indirizzo sotto riportato, selezionando il collegamento Download Root kitRevealer che troviamo sulla destra.

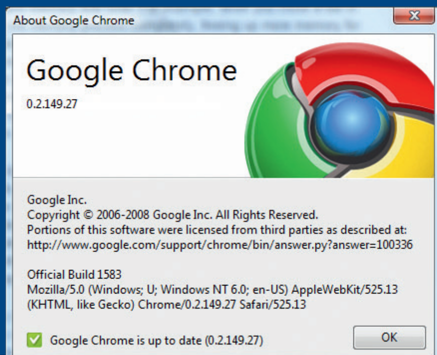
- PRODUTTORE: MICROSOFT
- HTTP://TECHNET.MICROSOFT.COM/EN-US/SYSINTERNALS/BB897445.ASPX

È l'ora di CHROME

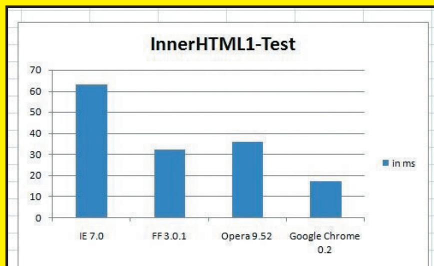
La grande G l'aveva promesso e l'ha fatto, ecco il browser di Google, IE e tutti gli altri tremano

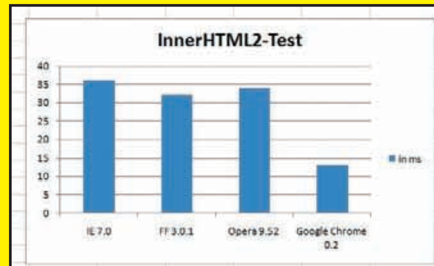
Chrome è stato progettato praticamente da zero, sfruttando Webkit (il tool open source già utilizzato in Safari), per rispondere meglio degli altri browser alle esigenze dei navigatori di oggi, abituati a interagire con applicazioni Web 2.0, a vedere video in streaming e a dover aspettare spesso troppo tempo su siti troppo pesanti anche con connessioni veloci. L'idea alla base è che si può migliorare di molto la resa dei siti web rendendo disponibile localmente una struttura più snella e efficiente che ottimizzi ad esempio il codice javascript utilizzato sempre di più (Gmail con Chrome vola che è un amore ad esempio) e che sia al contempo robusta e rapida al costo ovviamente di una maggiore quantità di ram richiesta. L'interfaccia si presenta completamente pulita, con solo i bottoni di navigazione e impostazioni e uno spazio URL che tramite il completamento automatico (denominato Google Suggest) basato sulla ricerca tra i siti preferiti e trasmissione dei dati direttamente a google (per cercarli su web) si può impostare la "rotta" di navigazione in un modo più naturale e sicuramente semplificato. E appena lanciato Chrome presenta di default come home-page i thumbnail degli ultimi siti visitati, la lista dei preferiti e in evidenza ovviamente una riga pronta per far ricerche su Google.

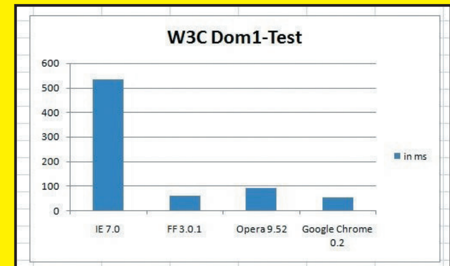


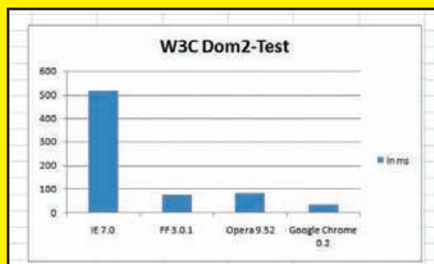


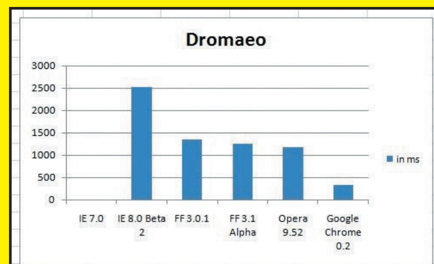
Ogni pagina web viene gestita come un processo applicativo separato, in modo che su eventuale crash (ad esempio di un'animazione flash) in una pagina non vengono compromesse le altre già aperte. Al contempo c'è un controllo sulla gestione della ram basata sulle moderne tecniche di protezione di memoria offerte dai sistemi operativi pre-emptive e multitasking. Letteralmente, per ogni nuovo tab aperto viene lanciato un nuovo processo che andrà a gestire la sua occupazione di memoria. Esiste anche un task-manager nascosto che può essere visualizzato cliccando con il tasto destro del mouse sulla barra dei tab in alto; altri menu di chiusura e reload delle schede si attivano cliccando sopra i tab aperti. Nel task-manager vengono visualizzati i processi di chrome in run (inclusi i plug-in come Flash) con la relativa occupazione di risorse ram e cpu. I tab sono dinamici e si possono trascinare fuori e dentro le finestre per renderli finestre autonome o riportarli dentro per farli diventare tab. E' possibile poi aprire le finestre nella modalità definita "In incognito", che non registra nessuna traccia relativa alla navigazione nel sito che si sta aprendo in questa modalità (ragioni di privacy). In questo caso verrà aperta una nuova finestra non trascinabile in quelle già aperte, con visualizzata l'icona esplicita di qualcuno vestito con impermeabile, cappello e

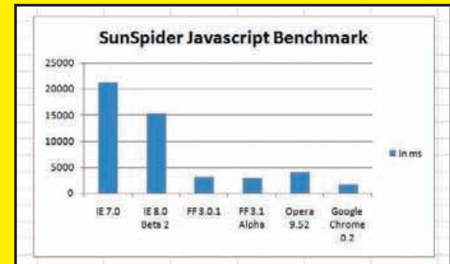






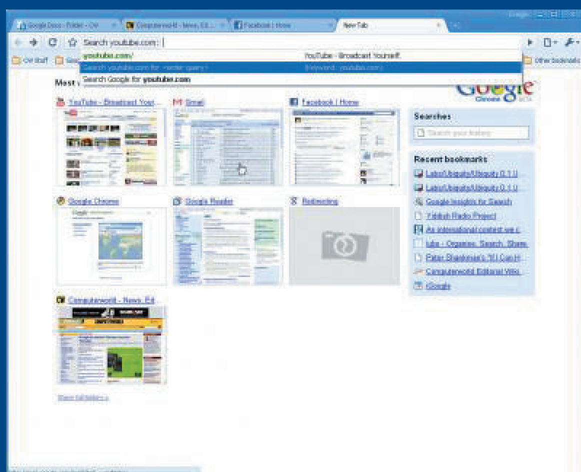






Ecco i test comparativi tra i vari browser presenti ora sul mercato e il nuovo nato di casa Google.

occhiali! Ma veniamo alla navigazione. La prima impressione che si ha è che effettivamente ci troviamo di fronte a un prodotto nuovo, magari più spartano, ma reattivo e soprattutto rapido nel rendering delle pagine. Ho fatto diverse prove andando ad aprire pagine più o meno cariche e solitamente tutte appaiono quasi subito senza gli abituali effetti di ritardo cui siamo abituati fin dagli albori del web (pagine e immagini caricate in successione, animazioni flash che fanno aspettare). Ad ogni modo, gli amici tedeschi di PCWorld si sono messi a far le pulci con diversi benchmark ed hanno effettivamente dichiarato Chrome come il browser più veloce sulla piazza (http://www.pcworld.it/showPage.php?template=Screenshots&id=277&cod=ga). Ma ci sono alcuni problemi di gioventà, come errori nella gestione di siti web avanzati tipo blogger (che è sempre di google!!!) nell'editing delle immagini nei post o in alcune applicazioni facebook (es. nel gioco Pirates). E i download sono estremamente semplificati (troppo): cliccando su un file viene direttamente avviato il download in una cartella Downloads e la barra resta in evidenza anche dopo il termine, senza richiedere alcun intervento all'utente (sarà interessante vedere quali protezioni contro i virus saranno implementate quindi).



Inoltre guardando alle connessioni che vengono aperte e dirette verso il dominio google.com ci si inizia a chiedere quanti siano in concreto i dati scambiati tra la nostra navigazione e il grande-fratello-google. Non sono quantificabili, dal momento che tra Google Suggest e la navigazione continuamente sotto controllo, si genera una quantità non rintracciabile di informazioni che arrivano fino a loro. Google dichiara di trattenere "solo" il 2% di queste informazioni, ma non sappiamo esattamente quali siano.

E' chiaro che avendo sviluppato una miriade di applicazioni per il web Google voglia ora affermare una posizione più importante di tali servizi ed è per questo che è sceso in campo riaccendendo la guerra tra i browser. E infatti a quanto ha affermato Sergey Brin, co-fondatore di Google, durante una conferenza stampa, è probabile che Chrome diventi il browser di default per Android magari con una versione apposita per dispositivi mobile. Staremo a vedere. Intanto limitiamoci a giocare con questa nuova creatura che potrebbe rivelarsi avere un lato oscuro difficilmente gestibile.
Ad esempio, chi farà tranquillamente home-banking con Chrome?

Massimiliano Brasile

Difendiamo il TORRENT

Anche se siamo in molti a scommettere su eMule e sul suo incredibile catalogo di file multimediali, BitTorrent sta conquistando sempre più adepti. Scopriamo qual è la forza di questo protocollo, che offre scaricamenti rapidi e di qualità...

Tutto ciò che abbiamo sempre desiderato sapere…
Programma e al tempo stesso protocollo per la connessione a una rete, BitTorrent è il parto di un informatico di genio, Bram Cohen. Quest'ultimo ha ideato il protocollo di condivisione e anche il programma che consente di utilizzarlo. Dal momento che alla sua nascita BtiTorrent era open source (il codice sorgente era cioè a disposizione di tutti e chiunque poteva crearne una propria "versione"), sono apparsi decine di nuovi programmi: µTorrent, Azureus, BitComet eccetera. Naturalmente, ciascuno offre vantaggi specifici: in un caso le dimensioni ridotte, in altri la presenza di parametri avanzati e così via. Lo stesso eMule consente oggi, mediante un semplice plug-in, di utilizzare questo protocollo P2P. Il suo funzionamento particolare fa sì che abbia una posizione a sé nell'universo peer-to-peer.

:: Come funziona?

Tutto ha inizio con la condivisione di un file. Un utente della rete crea un file .torrent dal file che desidera condivide-



re mediante il suo programma (o client). Questo file Torrent, che misura solo poche decine di kilobyte, contiene i meta-dati di quello da condividere: nome, dimensioni, indirizzo del computer che lo ospita e, soprattutto, le informazioni necessarie per individuare il tracker che gestisce caricamenti e scaricamenti. Il tracker è un server che inizializza lo scaricamento comunicando l'indirizzo dei computer sorgente (che contengono per intero o in parte il file desiderato) e che va collocato su un server dedicato. Ci sono centinaia di siti specializzati in questo tipo di servizio. La persona che desidera ottenere il file deve prima scaricare il Torrent e poi collocare questo piccolo file nel suo client Torrent. Sarà quest'ultimo programma a dare inizio allo scaricamento del file "vero". Notiamo che esiste anche un metodo senza tracker, completamente decentrato (più facile da utilizzare ma anche più "volatile").

VIDEO DAI NOMI ESOTICI

Sulle reti P2P e su BitTorrent in particolare, i video hanno titoli che possono creare confusione. In realtà, il loro scopo è fornire all'utente informazioni sulla natura e sulla qualità dei file da scaricare. Ecco una piccola traduzione:

> DivX o XviD: significa che il video è compresso nei formati corrispondenti. La qualità è elevata ma non pari a quella di un DVD.
> DVD o DVDR: Indica la copia di un DVD, senza alcuna modifica.
> CAM: Film registrato al cinema mediante videocamera; spesso è sinonimo di cattiva qualità.
> TS: Film registrato al cinema ma con una cura maggiore rispetto a un file CAM (treppiede, nessuno spettatore in sala ecc.)
> TVRip, SatRip, VHSRiP: File prelevato dalla TV, da un satellite o da una videocassetta.
> DVDSCR o Screener: Copia di un film in anteprima (video per giornalisti, per esempio). La qualità può oscillare da pessima a buona.
> HD: File ottenuto da una sorgente ad alta definizione.
> Sub: File di sottotitoli (formato SUB, SRT, TXT, SMI ecc.)
> VO, VI, VOST: Versione originale, versione italiana e versione originale con sottotitol

:: Perché un simile successo?

I file disponibili sulla rete BitTorrent sono di qualità elevata, i falsi sono rari e la velocità di scaricamento è generalmente alta (sebbene dipenda dal numero degli utenti interessati al file). Un client BitTorrent ben configurato consente velocità di scaricamento fino ai 300 KB/s se le fonti sono sempre disponibili. Dato il particolare funzionamento della rete, maggiore è la domanda relativa a un file, più alta è la velocità! La natura di questa rete fa sì che vi sia un gran numero di file recenti, mentre quelli più vecchi o meno richiesti finiscono per scomparire rapidamente. I releaser (cioè gli utenti che mettono a disposizione le ultime novità) scommettono molto su questo protocollo... Per il grande pubblico, il principale freno allo sviluppo della rete è costituito dal fatto che le ricerche non vengono effettuate mediante un motore integrato (sebbene qualcuno ci abbia provato) ma attraverso siti specializzati o cataloghi di ricerca. Tuttavia, BitTorrent comincia a farsi conoscere in tutta Europa.

:: Tracker e cataloghi: i siti della discordia

Il successo di BitTorrent è legato alla qualità dei siti e dei cataloghi che elencano i file Torrent. Questi ultimi, tra i quali abbondano naturalmente anche i siti illegali, sono l'obiettivo della polizia della Rete e delle major di ogni tipo...Per trovare dei file Torrent è indispensabile passare attraverso un tracker (un sito che reindirizza gli utenti gli uni verso gli altri). Naturalmente alcuni programmi, tra cui il client ufficiale, dispongono di motori di ricerca incorporati nell'interfaccia; si tratta però di semplici "scorciatoie" che rimandano a tracker "amici". All'interno di questa grande famiglia esistono tracker pubblici dai quali chiunque può scaricare (come The Pirate Bay) e tracker privati ai quali è necessario iscriversi (come SnowTigers) e a volte perfino farsi presentare da un membro.

:: Caccia al tracker

Infine, ci sono i cataloghi, come il famoso Mininova. Questi non si occupano dell'aspetto tecnico (archiviazione e interscambio dei file), limitandosi a recensire i collegamenti offerti da vari tracker allo scopo di metterne a disposizione il maggior numero possibile. Naturalmente, la scelta è vastissima, sebbene purtroppo a volte i collegamenti siano "morti" e possa trascorrere un certo tempo prima che l'amministratore li rimpiazzi. Per quanto riguarda i tracker, hanno tempi di reazione più ridotti, grazie alle loro solide comunità di fan. Infatti, i tracker comprendono nella maggior parte dei casi un forum in cui gli utenti discutono, collaborano e chiedono ad altri utenti il "re-seed" di specifici file Torrent, cioè chiedono loro di rimettere in attività il Torrent sorgente..Ovviamente, questi siti o cataloghi specializzati si attirano l'odio dell'industria degli audiovisivi. Alcuni hanno già subito pesanti sanzioni (come TorrentSpy, condannato a pagare 110 milioni di dollari di multa); altri sono in attesa di giudizio o sono oggetto di attacchi diretti. Per esempio, Mininova si è attirato recentemente gli strali della BREIN, l'equivalente olandese della SIAE. Dopo aver più volte chiesto una soluzione per il filtraggio dei collegamenti illegali su Mininova, l'associazione ha deciso di portare il sito in tribunale. I responsabili del tracker si difendono spiegando di aver sempre bloccato l'accesso a qualsiasi



LA TOP 5 DEI SITI BITTORRENT

Da questa tabella è facile capire non solo come i siti di collegamenti Torrent siano in ascesa ma anche come i primi cinque siano entrati tra i 500 siti più visitati al mondo...

POSIZIONE	SITO DI TORRENT	POSIZIONE DICEMBRE 07	POSIZIONE DICEMBRE 08	VARIAZIONE PERCENTUALE
1	MININOVA.ORG	63°	53°	+19
2	THEPIRATEBAY.ORG	182°	130°	+40
3	ISOHUNT.COM	170°	147°	+16
4	TORRENTZ.COM	231°	192°	+20
5	BTJUNKIE.ORG	689°	469°	+47

Fonte: Alexa. Classificazione dei siti più visitati al mondo.

Torrent su richiesta del rispettivo detentore dei diritti. A fronte dell'immenso traffico che percorre Mininova, tuttavia, la BREIN ha ritenuto insufficiente questa misura. Infine, per evitare guai, alcuni siti hanno preferito fare le valigie per trasferirsi sotto cieli più ospitali. È il caso di Demonoid, che ha definitivamente traslocato in Ucraina, Paese considerato meno severo nei confronti di questo tipo di attività.

:: Belle parole e denaro sporco?

Naturalmente, i siti sotto accusa protestano sostenendo di non ospitare nulla di illegale (il che è vero, dato che nella peggiore delle ipotesi ospitano file Torrent da poche decine di KB e, nella migliore, semplici collegamenti a questi ultimi) ma le major evidentemente non la pensano così. MPAA e compagnia ribattono che i tracker forniscono all'utente di Internet i mezzi per praticare la pirateria. Francamente, non si può negare che queste attività favoriscano la pirateria, dato che la maggior parte di questi siti fanno molta pubblicità sulle loro pagine. Sebbene in una recente intervista gli amministratori di The Pirate Bay ci abbiano risposto che questi introiti servono esclusivamente a pagare i server e le spese generali, c'è di che dubitarne. Cinque di questi cataloghi/tracker figurano tra i 500 siti più visitati del mondo (si veda la nostra tabella) e i profitti da loro generati dovrebbero ammontare solo a qualche migliaio di dollari? Impossibile! Basta considerare la velocità con cui Demonoid ha riaperto i battenti dopo il suo primo scontro con la BREIN e la ricerca sfrenata di nuovi server in Ucraina per capire che questi siti fanno un sacco di soldi. Insomma, ci sarebbe qualche riflessione da fare sulla veridicità delle belle parole di condivisione e diritto alla cultura fatte proprie dai principali interessati…

:: Piccoli rivoli formano un grande fiume

Da quando il marchio BitTorrent ha deciso di diventare integerrimo, il sito www.bittorrent.com non contiene più alcun collegamento illegale. Si è invece trasformato in un vero e proprio punto di riferimento per i video on-demand via Torrent. Ci troveremo dunque film, documentari e manga ma per ottenerli sarà necessario passare alla cassa. È possibile acquistare o noleggiare i file, che purtroppo contengono DRM… Sempre nell'ambito del contenuto legale al 100%, citiamo http://beta.legaltorrents.com e www.publicdomaintorrents.com. Questi siti offrono Torrent caduti nel pubblico dominio (vecchi film o contenuti generosamente offerti dai detentori dei diritti) o che ricadono sotto la licenza Creative Commons: videogiochi, documentari, audiolibri eccetera.Per gli appassionati dell'e-learning (cioè "didattica elettronica"), anche il sito http://docs.torrents.ro è particolarmente interessante. Dato che i tracker sono molto numerosi, alcuni hanno deciso di specializzarsi in un ambito preciso. È il caso di www.serie-torrent.com, che propone serie TV, o di www.anime-torrent.org, specializzato nei cartoni animati giapponesi. Infine, esiste un settore in grande espansione, quello degli iPod e dei telefoni cellulari. In effetti, è molto complicato per un utente utilizzare DivX non ottimizzati per il suo dispositivo (difficoltà di codifica eccetera). Per questo www.podtropolis.com e www.ipodnova.net offrono contenuti rigorosamente selezionati per i fan dei cellulari e dei dispositivi portatili.



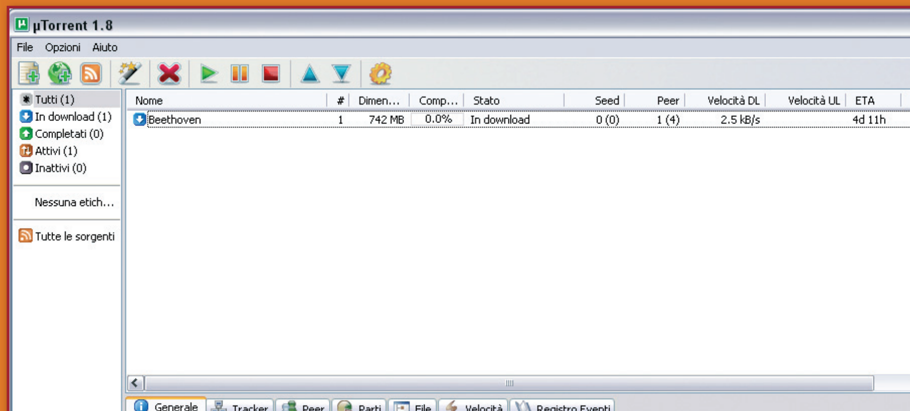
µTorrent, niente di meglio

Nella giungla dei client BitTorrent, pochi riescono a fare bene il loro lavoro come uTorrent. Lasciamoci tentare da questo client ricco di funzionalità che non appesantirà il nostro sistema mantenendo alta la nostra velocità di scaricamento

Con il suo peso piuma e il consumo ridotto delle risorse di sistema, µTorrent è ideale per le configurazioni non troppo potenti e per chi vuole evitare sprechi. La sua interfaccia è priva di fronzoli e tutte le funzioni essenziali sono accessibili con un clic. Certamente ha meno funzionalità di altri programmi come per esempio Azureus, ma non è certo meno efficiente: le velocità e la gestione dei trasferimenti sono impressionanti. Esiste anche una versione di µTorrent che non richiede installazione per funzionare, caratteristica molto pratica per averlo sempre con noi, su una chiave USB per esempio. Questo client saprà certamente conquistare sia i principianti sia gli utenti avanzati. Scopriamo senza indugiare oltre i migliori trucchi per sfruttare il suo potenziale e intraprendere l'avventura BitTorrent senza paura.

:: Configurare

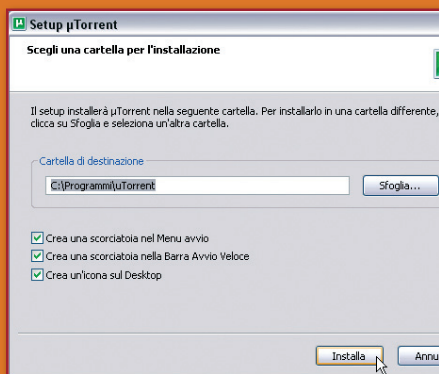
Avviamo l'eseguibile poi, nella finestra che si apre, scegliamo le opzioni che ci interessano. Per modificare eventualmente la lingua dell'interfaccia, clicchiamo su Opzioni > Impostazioni > Generale e scegliamo quella che preferiamo nel menu che compare. Se usiamo un firewall, controlliamo subito se quest'ultimo accetta µTorrent, altrimenti creiamo una regola filtro per autoriz-



INFO UTILI

Nome: µTorrent
Dove lo trovo: www.utorrent.com
Versione: v1.8 Stable
Dimensioni: 0.26 MB
Lingua: Italiano
Licenza: Gratuito

zare il collegamento. Anche se non è affatto obbligatorio, se usiamo un router possiamo sfruttare l'interfaccia di gestione per aggiungere un numero di porta identico (superiore a 15000) per il traffico in entrata e in uscita e indicare l'indirizzo IP del PC e il protocollo TCP o UDP. Nella scheda Connessione di µTorrent controlliamo che la porta corrisponda a quella indicata nel nostro router e soprattutto non selezioniamo la voce Sel. Casuale della porta a ogni avvio. Consiglio valido anche per un firewall.



:: Scaricare

Per specificare la cartella di destinazione dei file da scaricare, apriamo nelle Impostazioni la scheda Cartelle, selezioniamo la voce Metti i nuovi download in e clicchiamo sul pulsante Sfoglia rappresentato da tre puntini.

:: Trovare un file

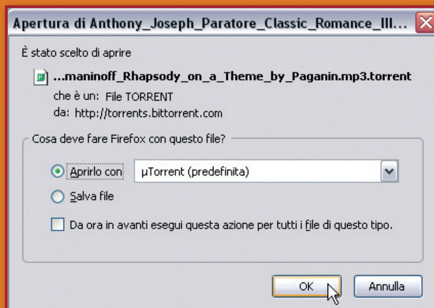
Per trovare un documento, un video, un programma o un MP3, il metodo più semplice consiste nello scrivere un nome di file nel campo Ricerca (in alto a destra) per poi scegliere un motore di ricerca fra Google e BitTorrent e confermare la nostra scelta. Premiamo infine il tasto Invio. I risultati verranno visualizzati in una pagina Web. Scegliamo il file che ha il numero di Seed (cioè i proprietari del file completo) più alto.

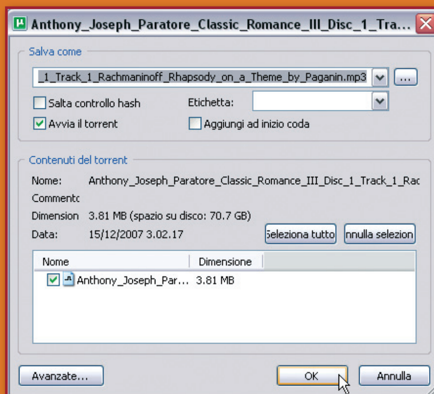
:: Scaricare direttamente...

Una finestra ci chiederà allora di aprire questo file con µTorrent o di scaricarlo sul nostro disco fisso. È più semplice aprirlo direttamente. µTorrent caricherà allora l'informazione contenuta in questo "tracker" e avvierà lo scaricamento del file finale. Quest'ultimo sarà più rapido se µTorrent troverà numerose fonti.

:: ... o più tardi

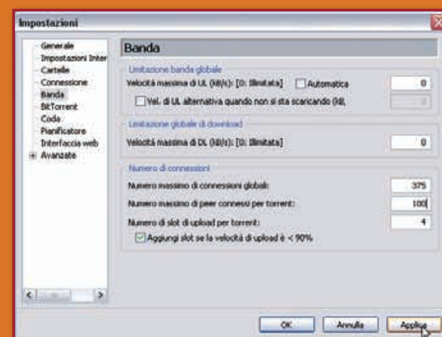
Possiamo anche salvare il nostro "tracker" .torrent: questo non contiene il file finale che stiamo cercando ma tutte informazioni che permetteranno di recuperarlo in un secondo tempo. Dovremo cliccare sull'icona Aggiungi Torrent in alto a sinistra nella finestra del programma. Nella finestra che si apre clicchiamo sul nostro file .torrent e poi su Apri. Nella nuova finestra lasciamo selezionata l'opzione Avvia il torrent e clicchiamo sul pulsante OK per avviare lo scaricamento.



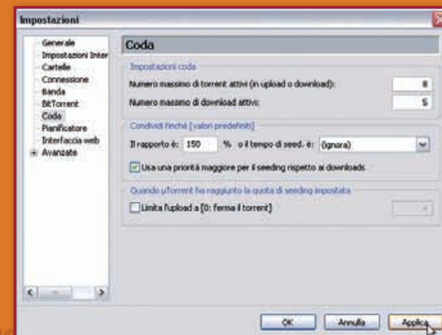


:: Impostazioni

Per migliorare le prestazioni di scaricamento, possiamo modificare alcuni valori predefiniti nella scheda Banda, accessibile dalle Impostazioni. Possiamo aumentare il numero massimo di connessioni globali a 375 e il numero massimo di client per torrent a 100. Se ci accorgiamo di un rallentamento, possiamo sempre ristabilire valori predefiniti: 200 per il primo parametro e 50 per il secondo. Nella scheda BitTorrent possiamo anche selezionare senza rischi le voci che riportando l'indicazione DHT. Il DHT (che sta per Distributed Hash Table) permette l'identificazione delle diverse parti di un file presenti su una rete P2P.



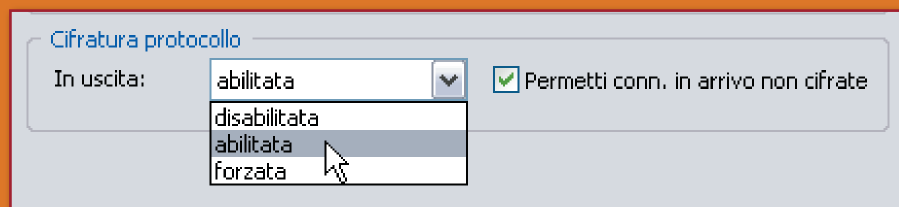
Queste informazioni sono necessarie quando usiamo µTorrent per creare un file .torrent a partire da un file salvato nel nostro computer. Questo non ha alcuna incidenza sui nostri upload e download. Per portare al massimo le prestazioni è necessario impostare la cosiddetta coda. Per aumentare il nostro rapporto è importante favorire l'upload a scapito del download selezionando la voce Usa una priorità maggiore per il seeding rispetto ai downloads nella scheda Coda. È una delle regole d'oro del P2P: condividere molto per scaricare più rapidamente. Nelle opzioni della Coda, definiamo un numero ragionevole di download attivi: 7 è un buon compromesso per evitare che



il nostro rapporto di trasferimento non subisca tracolli. Siamo modesti!

:: Sicurezza e anonimato

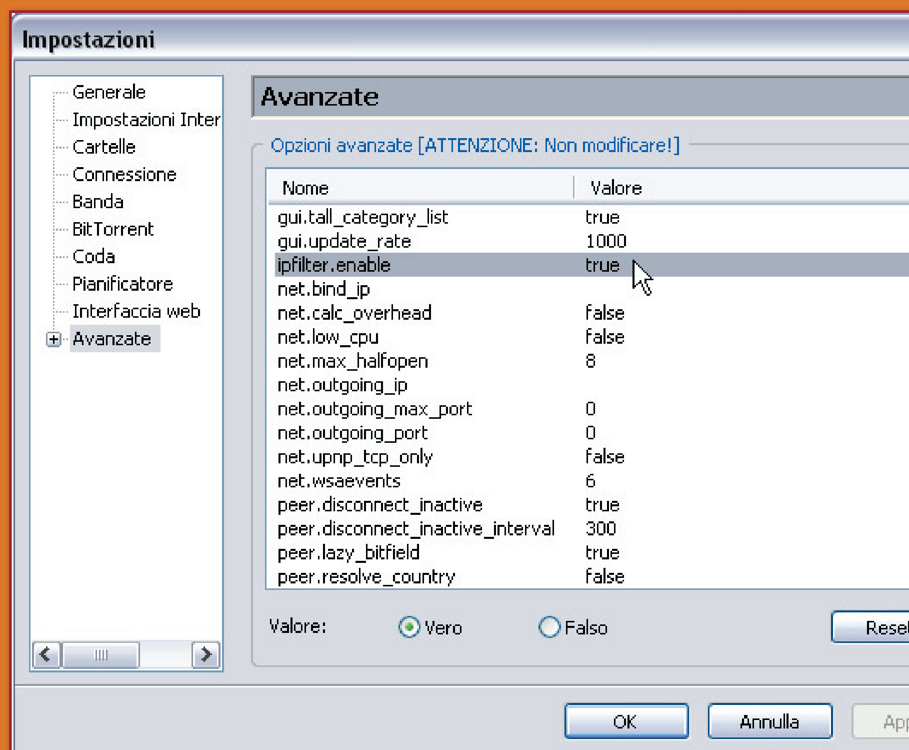
Il nostro fornitore di accesso a Internet potrebbe sorvegliare i protocolli utilizzati nel P2P e così limitare la velocità di scaricamento dei file. Per questo motivo, µTorrent propone un protocollo di criptazione dei collegamenti in entrata e in uscita. Questa procedura ha lo scopo di ingannare il dispositivo d'individuazione del protocollo.



Per attivarlo, nel menu Strumenti clicchiamo su Impostazioni e poi selezioniamo la scheda BitTorrent. Basta scegliere Attivo nel menu Cifratura protocollo e selezionare la voce Permetti conn. in arrivo non cifrate.

:: Gli spioni là fuori

Per garantirci più anonimato, come succede con eMule o Shareaza, possiamo usare il filtro di indirizzi IP in modo da bloccare gli IP indesiderabili (quelli dei PC spioni). Per farlo apriamo la seguente cartella nel nostro computer: C:\Documents and Settings\nome_utente \ Dati applicazioni \ uTorrent.
Scarichiamo l'elenco di filtri da www.bluetack.co.uk/config/nipfilter.dat.gz e decomprimiamolo nella cartella appena aperta. Rinominiamolo poi nipfilter.dat in ipfilter.dat. Accediamo alle impostazioni di µTorrent, nella scheda Avanzate cerchiamo l'opzione ipfilter.enable e assicuriamoci che il suo valore sia true. Se la modifica è andata a buon fine, dovremmo vedere un messaggio che indica che il filtro IP è stato caricato nella scheda Registro eventi.

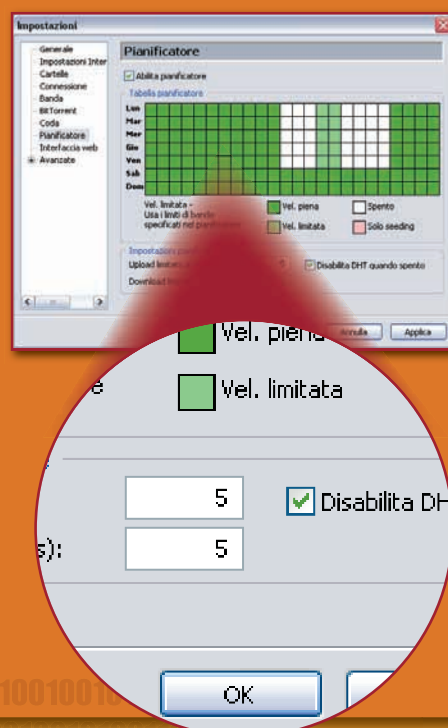


TRUCCO

µTorrent mette a disposizione WebUI, un modulo aggiuntivo che ci permette di controllare i nostri trasferimenti a distanza a partire da un altro PC. Se siamo abituati a usare gli Smartphones, Palm o Pocket PC proviamo µTorrent mUI, scaricabile dal sito www.utorrentmui.com.

:: Pianifichiamo i nostri scaricamenti

Il pianificatore è molto utile per ottimizzare lo scaricamento e controllare la banda occupata. Attiviamolo accedendo alle Impostazioni: clicchiamo sulla scheda Pianificatore e selezioniamo la voce Abilita pianificatore. Si presenta sotto forma di una griglia che mostra a sinistra i giorni della settimana. Basta cliccare su ogni casella per modificarne lo stato. Il bianco impedisce ogni collegamento, il verde chiaro limita le velocità di trasferimento e il verde scuro indica che non c'è alcun limite. Applichiamo le nostre impostazioni e confermiamo cliccando su OK. ■



La chiave d'avvio

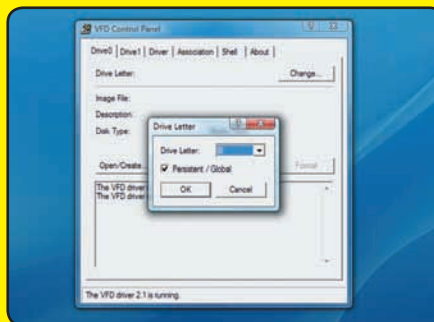
Non ho il floppy e i miei driver mi richiedono l'avvio da dischetto, come la posso risolvere??? Con una chiave USB

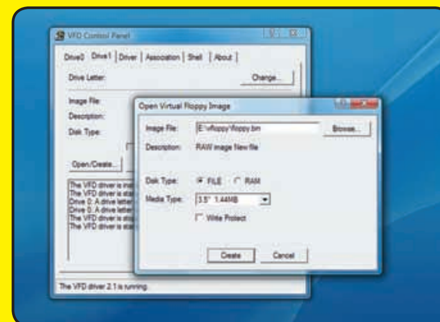


Fino a qualche anno fa tutti i PC avevano un lettore di floppy disk. La limitata capienza di questi supporti, solo 1,44 MB, si è tuttavia fatta troppo restrittiva per qualsiasi applicazione moderna, per cui sono sempre di più i produttori che decidono di non installare più questo vecchio dispositivo.

CREIAMO UNA CHIAVE



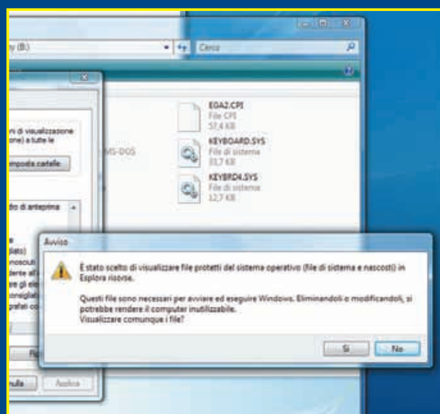




1 AVVIAMO VFD CONTROL PANEL
Una volta estratto l'archivio di VM Back in una cartella a piacere, per esempio E:vfloppy, occorre avviare il programma vfdwin.exe. Nel pannello Driver, facciamo clic su Start.

2 CREIAMO L'UNITÀ VIRTUALE
Se nel nostro PC manca del tutto un drive per i floppy, possiamo scegliere indifferentemente le unità Drive0 o Drive1, se già c'è, meglio scegliere Drive1. Dobbiamo assegnare una lettera di unità: meglio B.

3 ECCO IL FLOPPY VIRTUALE
Una volta creato il drive, occorre fare altrettanto con il floppy inserito al suo interno. Dal pannello Drive facciamo clic su Open/Create ed, eventualmente, impostiamo un percorso e un file immagine.



Per creare una chiave USB avviabile, dobbiamo cambiare le impostazioni relative alla visualizzazione dei file nascosti dal menu Finestra (Windows 2000/XP) oppure Organizza (Vista).

Eppure, ancora oggi ci sono operazioni che richiedono un riavvio del computer in "modalità DO S", come per esempio l'aggiornamento del BIOS della scheda madre.

In casi come questo, con i software opportuni, una chiave USB può sostituire le funzioni del vecchio dischetto di avvio.

:: Che cosa serve

Ci servono tre cose: una chiave USB, possibilmente di piccole dimensioni – magari quel vecchio modello da 64 MB che giace inutilizzato da qualche anno in un cassetto della scrivania – un floppy d'avvio e il programma HP USB Disk Storage Format Tool, che possiamo scaricare dal sito http://snurl.com/2zip6 e che si occuperà di trasferire i file d'avvio necessari dal floppy alla chiave di memoria, dopo averla formattata.
Dato che non abbiamo un lettore di dischetti dobbiamo "emulare" il floppy un driver apposito. Sul sito http://chitchat.at.infoseek.co.jp/vmware/vfd.html è possibile trovare VM Back, un'applicazione che consente di aggiungere un floppy "virtuale", più o meno come fanno certi programmi con i dispositivi ottici. Dopo aver scaricato il file .zip che contiene VM Back e averne estratto il contenuto, per attivare il driver dobbiamo lanciare il programma vfdwin.exe. Una volta creata la nostra unità, dovremo assegnarle una lettera di unità (per esempio B:), creare un floppy virtuale – mantenuto nella RAM o su un file immagine – e quindi formattarlo tramite Risorse del computer, selezionando l'opzione per creare un disco di sistema.

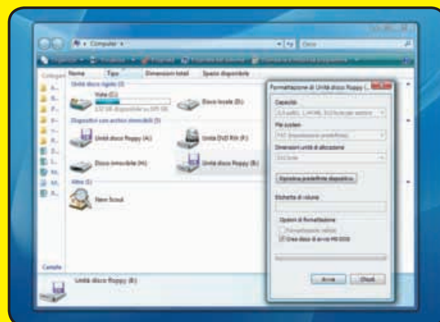
:: Avvio con la chiave



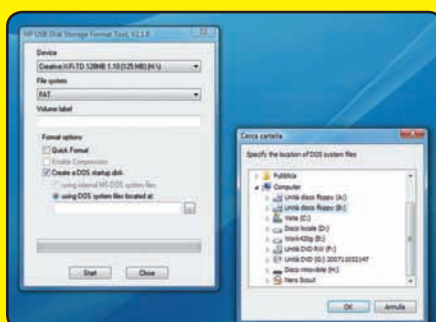
Dopo aver formattato il dischetto virtuale, dovremo lanciare il programma HP USB Disk Storage Format Tool e formattare la chiave di memoria, indicando il percorso del nostro floppy d'avvio (nel nostro caso, l'unità virtuale B:).

Dopo qualche secondo la chiave sarà pronta, e non ci resterà altro da fare che copiare i file rimanenti dal dischetto alla chiave USB, compresi tutti i programmi che ci servono per l'aggiornamento del BIOS o per la manutenzione del computer. Al riavvio, il BIOS dovrà essere configurato per consentire l'avvio del sistema da una periferica USB: facciamo riferimento al manuale d'uso della nostra scheda madre per capire come impostare le opzioni del BIOS. ■

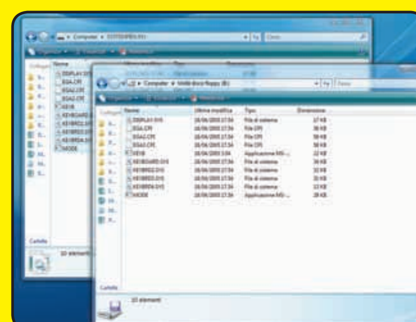
D'AVVIO CON VM BACK



4 FORMATTIAMO IL DISCHETTO
Da Risorse del computer, facciamo clic con il tasto destro del mouse sull'icona del drive B e scegliamo Formatta. Selezioniamo Crea disco di avvio MS-DOS e avviamo la procedura.



5 PREPARIAMO LA CHIAVE
Con il programma di formattazione di HP, selezioniamo la chiave, il file-system FAT e l'opzione Create a DOS startup disk using DOS system files located at. Premiamo [...] e scegliamo l'unità floppy B:\.



6 COPIAMO I FILE NECESSARI
Copiamo tutti i file da B:\ alla chiave appena formattata e rispondiamo NO a ogni eventuale richiesta di sovrascrittura. Copiamo anche gli altri file e i programmi che ci servono.

DRM... li conosco, li odio !!!

Vera croce di tutti gli appassionati di musica digitale, manette ai polsi dei nostri file, scopriamo come funzionano



A cosa serve realmente? Questa è la domanda che in molti si pongono quando scoprono che i loro file MP3, regolarmente comperati tramite uno dei tanti negozi Internet, contengono al proprio interno un marcatore DRM.
In effetti si tratta di un dubbio legittimo visto che, solitamente, acquistando un oggetto se ne diventa automaticamente proprietari. Eppure, nel caso dei file MP3 e non solo, non sempre è così: la tecnologia DRM, infatti, serve proprio a stabilire limiti e modalità di utilizzo di quello che, a prima vista, sembrerebbe già nostro.

:: Questione di interpretazione

Con la sigla DRM, cioè Digital Rights Management, viene definito un insieme di tecnologie che servono per il controllo e la tutela del diritto d'autore. Spesso, per indicarle, viene usato anche il termine di filigrana digitale.
Il motivo è semplice: come la filigrana inserita all'interno delle banconote ne impedisce la falsificazione, così la tecnologia DRM aggiunge al file sul quale viene applicata, una serie di informazioni nascoste che ne regolamentano l'utilizzo. In pratica, quindi, acquistando un file con certificazione DRM, non compriamo il file stesso ma solo il diritto di poterlo riprodurre con le limitazioni imposte dall'azienda, o dal rivenditore, che ce lo ha venduto.
Le principali applicazioni del DRM sono tre: la certificazione di proprietà, il controllo d'accesso e infine, il controllo delle copie illegali. All'interno dei marcatori DRM, comunque, possono essere inserite ulteriori limitazioni differenti sia in base alla modalità di distribuzione, sia alle logiche di chi detiene effettivamente i diritti d'autore sul contenuto.

:: Facciamo chiarezza

Ognuna delle tre modalità principali di utilizzo della filigrana digitale serve a uno scopo ben preciso.
La certificazione di proprietà permette di identificare la copia originale e quindi l'eventuale derivazione illegale, di un qualsiasi file musicale. Nei file audio, prima di essere trasformati nel formato compresso MP3, viene inserita un'informazione aggiuntiva sui diritti d'autore grazie a una specifica tecnica che prende il nome di PCM Watermarking. Nel caso del controllo d'accesso, invece, al file audio originale, tramite una diversa tecnologia che prende il nome di Bitstream Watermarking, viene aggiunto uno speciale marcatore che ne garantisce l'originalità. Il file così trattato può essere riprodotto solo sui lettori che sono in grado di riconoscere le informazioni di codifica e solo per il numero di volte specificato dal contratto che abbiamo sottoscritto al

L'arte della SICUREZZA

Tre ottimi tools per la sicurezza del nostro pc con il Pinguino



La sicurezza informatica non è un prodotto che si può comprare in "scatola" ma è piuttosto un processo continuo e articolato.

La colonna portante di questo processo è la conoscenza. Non si può infatti pensare seriamente di gestire la sicurezza di un complesso informatico, sia esso un singolo server che una farm, se non si conoscono i principi fondamentali sui cui si fondano i sistemi operativi e le comunicazioni in rete. Bisogna quindi studiare la struttura del proprio sistema operativo e la teoria delle reti, con particolare attenzione alla gerarchia ISO OSI. Si deve poi inquadrare il TCP/IP entro il modello OSI e capire come è stato implementato all'interno del sistema operativo in uso. In Rete ci sono, a questo proposito, molti ottimi libri e tanta documentazione tecnica di qualità. L'acquisizione delle nozioni è a sua volta un processo continuo. Lo studio deve infatti protrarsi per tutto l'arco della propria carriera tecnica, secondo il principio che in informatica si impara qualcosa ogni giorno ma non si impara mai a sufficienza. La conoscenza teorica diventa in questo contesto uno strumento per valutare l'affidabilità delle configurazioni presenti presso i propri sistemi. Si possono infatti avere sistemi di qualità, costantemente aggiornati, ma configurati in maniera poco attenta. Spesso inoltre si compiono in buona fede errori o sviste che possono rivelarsi fatali. Per mitigare queste situazioni esistono strumenti di monitoraggio e controllo delle reti e dei sistemi. Attraverso questi sistemi si possono eseguire scansioni o analisi passive per meglio valutare lo stato dei server in propria gestione. Si vedranno in questo tutorial tre strumenti di grande fama, utilizzati dai professionisti dell'informatica e delle reti per eseguire valutazioni sul campo.
Tutti gli strumenti presentati hanno il vantaggio di essere multipiattaforma, permettendo così l'uso su Linux, su Mac e su Windows.

NMAP

Uno degli strumenti più accreditati per l'analisi della sicurezza dei sistemi è Nmap (http://nmap.org). È un network scanner aperto, scritto originariamente da Gordon Lyon. Il suo scopo è eseguire una scansione di una sottorete o di un singolo sistema ed elencare i servizi accessibili dall'esterno su tale sistema. È una funzionalità oramai comune e presente su una grande quantità di tool analoghi. Ciò che differenzia Nmap dalla massa è l'uso raffinato che l'autore ha fatto della propria conoscenza dei protocolli Internet per implementare capacità di scansione superiori. Lo strumento non si limita quindi a verificare le porte aperte o chiuse presso i sistemi rilevati, ma applica piuttosto dei meccanismi di analisi per dedurre il tipo di sistema installato e per scoprire se vi sono servizi attivi che non divulgano la propria presenza. Per realizzare questo scopo vengono esaminati parecchi dettagli che gli standard tecnici (RFC) lasciano a discrezione dell'implementazione. Il differente modo in cui questi dettagli sono stati implementati dai produttori di software fornisce indizi molto utili a Nmap. Utilizzando Nmap verso i propri sistemi è possibile verificare la quantità di informazioni che vengono divulgate al mondo esterno e si possono così prendere appositi provvedimenti. Nmap dovrebbe essere utilizzato solo per sondare sistemi sotto la propria gestione. L'utilizzo dello strumento verso altri siti potrebbe costituire una violazione penalmente perseguibile.

1 La prima analisi che è importante eseguire è capire quante informazioni vengono divulgate al mondo esterno circa i modelli di apparati che sono utilizzati presso la propria installazione. Nonostante le password sicure e l'aggiornamento del sistema operativo è bene ridurre le informazioni divulgate. Un cracker a conoscenza del modello di apparato e della versione del firmware potrebbe accedere ai bollettini pubblici di sicurezza per scoprire eventuali vulnerabilità "forzabili" nell'apparato. La sequenza da usarsi su Nmap è la seguente: nmap -O -v <indirizzo IP>. Il parametro -O (O maiuscolo) esegue la rilevazione del sistema operativo, mentre il parametro -v attiva l'output "verbose". La scansione ha in questo caso "indovinato" che si tratta di un firewall Cisco Pix, con versione software 5.x o 6.x. Inoltre sono state rilevate le porte 22 e 443 aperte.

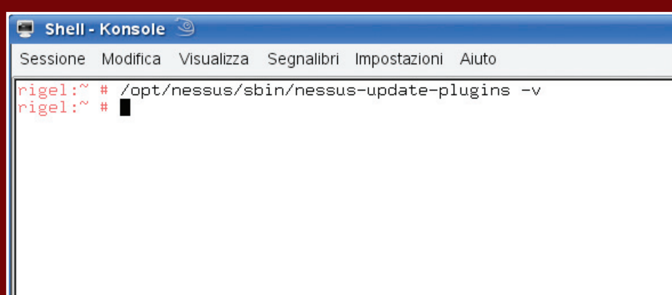
2 Una volta determinato il tipo di sistema e la versione del software a bordo, può essere utile comprendere quali porte sono aperte e quali informazioni sulle medesime sono disponibili al mondo esterno attraverso un meccanismo di scansione. La sequenza da utilizzarsi è la seguente: nmap -sV -v <indirizzo IP>. Il parametro -sV esegue una scansione delle porte aperte con lo scopo di determinare il servizio presente e la versione del software. La lunghezza della scansione può variare parecchio a seconda del tipo di apparato che si sta analizzando. Può trattarsi di un'operazione da pochi secondi come pure una procedura lunga diversi minuti.

3 Gli strumenti di scansione più comuni eseguono un controllo attraverso i ping, elencando semplicemente le macchine che hanno risposto al messaggio ICMP. Questa scansione è semplicistica in quanto ICMP ha solo uno scopo di gestione e di segnalazione, capace solo di evidenziare solo se l'host è attivo o meno. Come se non bastasse, è usanza sempre più diffusa disattivare la risposta ai ping, invalidando di fatto la scansione. Per avere una scansione di qualche utilità si dovrebbe controllare il protocollo TCP, per esempio con questa sequenza: nmap -sS -v <indirizzo IP>. Il parametro -sS esegue una scansione TCP utilizzando il bit SYN. Viene in pratica richiesta all'host in scansione l'apertura di una sessione TCP verso una particolare porta. L'host remoto risponderà in tal caso con un ACK. A questo punto Nmap non chiuderà il protocollo di iniziazione della sessione TCP. A seconda di come l'host in scansione risponderà al SYN iniziale di Nmap si otterranno informazioni circa lo stato della porta che si sta verificando (aperta/chiusa/stealth).

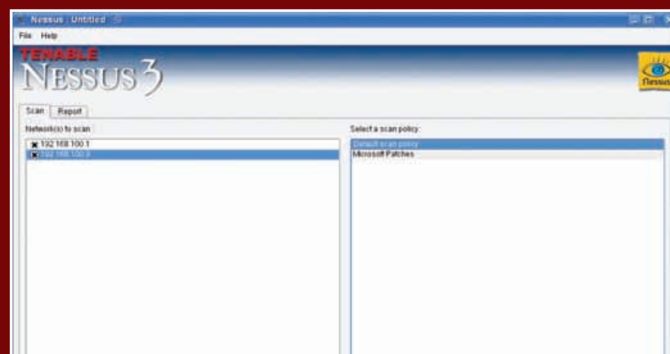
4 Non bisogna dimenticare che esiste anche il protocollo UDP e che potrebbero essere attive porte UDP con servizi critici violabili da cracker esterni. Per lanciare una scansione UDP si deve usare questo comando: nmap -sU -v <indirizzo IP>.
Questa forma di scansione è molto più lunga della sua controparte TCP. È possibile combinare le scansioni in una solo riga di comando: nmap -sU -sS -v <indirizzo IP>. Se si desidera invece eseguire una scansione di una intera sottorete, invece che di un singolo host, si deve usare questa sintassi: nmap -sU -sS -v <range>. Come in questo esempio di scansione complete della sottorete 192.168.100.n: nmap -sU -sS -v 192.168.100.1-254.

NESSUS

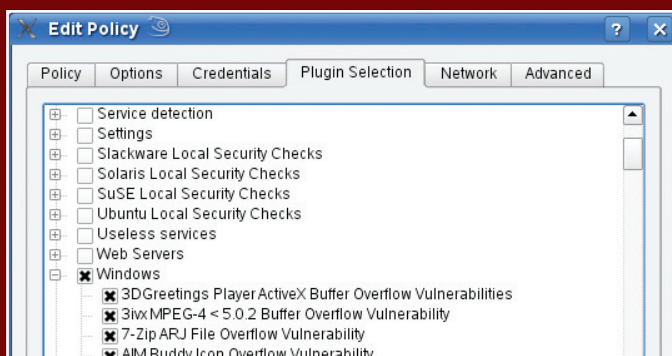
Nessus (www.nessus.org/nessus) è uno strumento di scansione e di analisi dei sistemi online. Il software è disponibile per Linux, BSD, Solaris, Mac OS X e per Windows in licenza GPL fino alla versione 2. Dall'attuale versione 3 il programma è diventato a tutti gli effetti commerciale. È garantito però l'utilizzo gratuito per l'utenza domestica e non commerciale, per gli enti di beneficenza e per il settore educativo. Nessus è in grado di eseguire la scansione delle porte aperte presso un singolo host o su una sottorete IP ma è in grado anche di controllare vulnerabilità software, problemi di configurazioni dei servizi e verificare la presenza delle patch aggiornate. Questa operazione è eseguita attraverso un database di "firme" che vengono costantemente aggiornate dalla case madre del prodotto. Queste sono caricate localmente e poi applicate al prodotto. Il pagamento della quota richiesta dalla software house permette proprio di usufruire di questo database di vulnerabilità per l'analisi dello stato dei sistemi. Nessus è composto da un componente server che opera in modalità di servizio e da un front-end grafico per l'uso intuitivo del prodotto. Nessus dovrebbe essere utilizzato solo per sondare sistemi sotto la propria gestione.
L'utilizzo dello strumento verso altri siti potrebbe costituire una violazione penalmente perseguibile.



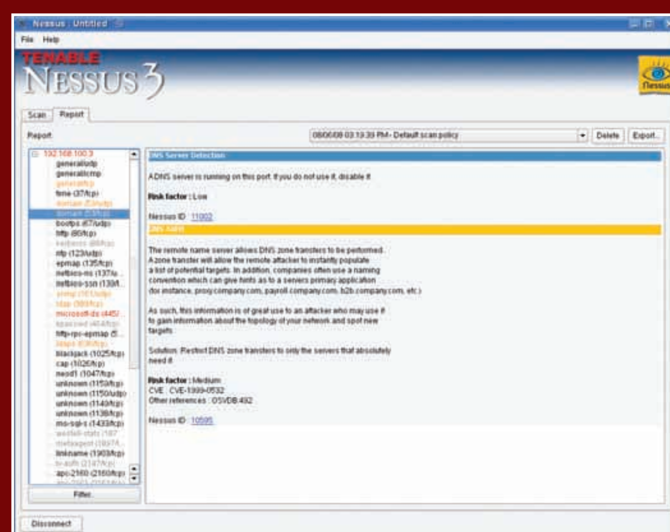
1 Se si intende utilizzare Nessus per monitorare regolarmente lo stato dei sistemi presso la propria organizzazione, è fondamentale che le "firme" siano costantemente aggiornate. Per realizzare questo scopo è necessario avere un codice di attivazione valido e fornirlo al sistema attraverso questa sequenza: /opt/nessus/bin/nessus-fetch --register <codice>. Dove <codice> è la chiave di attivazione recapitata viene e-mail dalla casa madre. La registrazione comporterà un primo download dei plug-in aggiornato. In seguito è necessario pianificare con regolarità il download degli aggiornamento attraverso questa sequenza: /opt/nessus/sbin/nessus-update-plugins.



2 Il client grafico di Nessus è composto da due linguette. Dalla prima linguetta si configura la scansione mentre dalla seconda, Report, si osserva il risultato delle operazioni. Il primo passo consiste nel premere sul pulsante + presente in basso a sinistra e indicare quale sistema o quale sottorete si vuole scandire. Poi si clicca su Scan now e si passa alla linguetta Report per osservare il risultato.



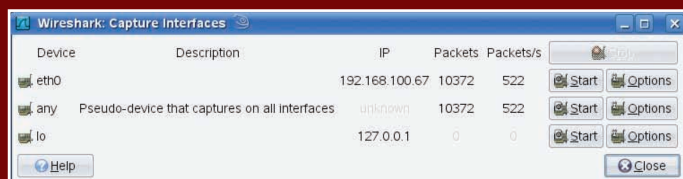
3 Prima di attivare una scansione si dovrebbe anche selezionare un "profilo". La potenza di Nessus sta infatti nella grande quantità di verifiche che è in grado di operare su diversi livelli della pila OSI. Oltre a uno sterile elenco di macchine e apparati, il programma segnala bug, vulnerabilità attive e problemi di configurazione. Si possono scegliere tra i due profili di default presenti oppure crearne dei nuovi premendo il pulsante +. Comparirà così una dettagliata finestra di configurazione. Dalla linguetta Plugin selection si potranno attivare i filtri specifici di controllo. Sono centinaia, in continua espansione, suddivisi per categorie quali per esempio Cisco, Windows, AIX, Debian, ftp, database, CGI, backdoor, ecc.



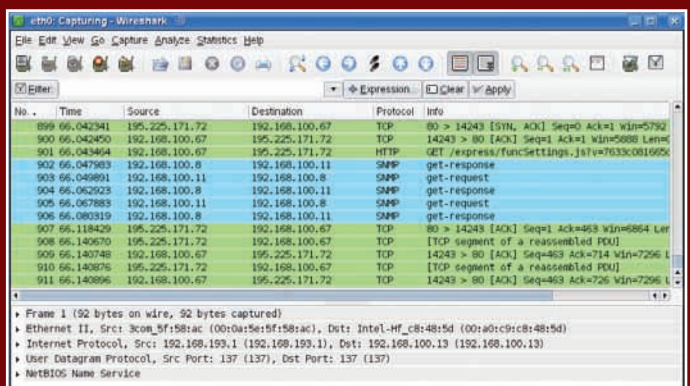
4 Una volta completata la scansione sarà presentata una finestra di commento, con consigli per il miglioramento della configurazione per ogni vulnerabilità rilevata.

WIRESHARK

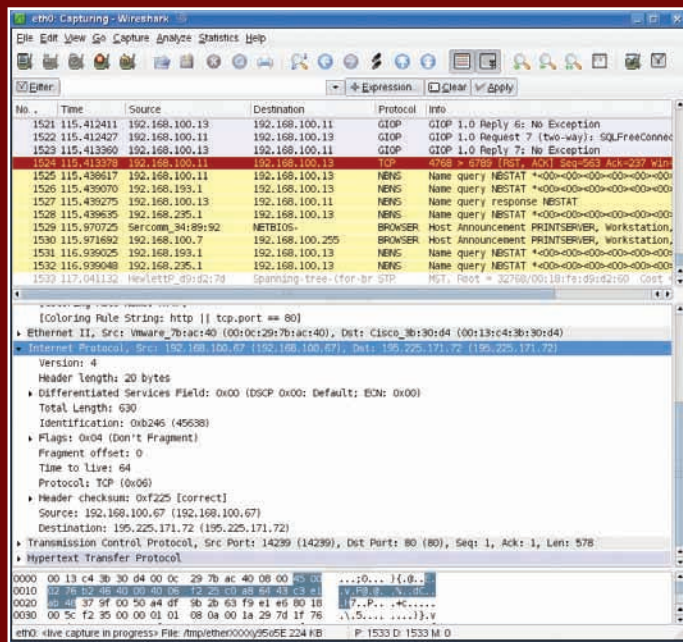
Wireshark (www.wireshark.org) è un analizzatore di protocollo aperto rilasciato in licenza GPL. Si tratta di un programma che si pone in ascolto sul canale dati locale e capta tutto il traffico in transito, mostrandolo a video in formato testuale. Per eseguire questa funzionalità, il software imposta la scheda di rete in modalità promiscua, condizione necessaria per l'elaborazione di comunicazioni non indirizzate alla macchina locale. Naturalmente è possibile monitorare solo le comunicazioni che sono visibili sul proprio canale di rete. Se il computer è connesso a uno switch, non si potranno vedere le comunicazioni che interessano le altre porte, in quanto isolate da un punto di vista hardware (a eccezione dei broadcast). Per visionare tutto il traffico è necessario avere uno switch managed e impostare la duplicazione di tutto il traffico verso la porta alla quale è connessa la propria macchina. La potenza del prodotto non sta nella facoltà di sniffing della rete, caratteristica erogata anche da altri programmi, ma dalla grande quantità di strumenti di analisi attraverso cui è possibile monitorare singole conversazioni o singoli protocolli, seguire le tracce temporali dei protocolli, filtrare il traffico, mettere in relazione le comunicazioni nel tempo, generare grafici, visualizzare gli interlocutori per protocollo, eseguire analisi sui pacchetti, salvare porzioni di traffico, ecc. Wireshark dovrebbe essere utilizzato solo per sondare sistemi sotto la propria gestione e compatibilmente con la policy aziendale sulla privacy. lxp

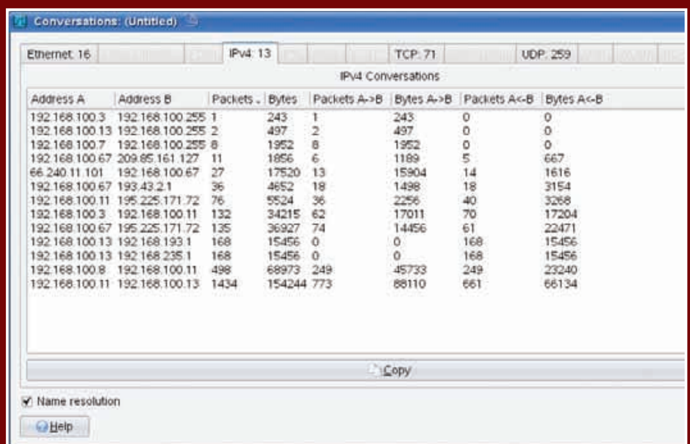


1 Per attivare il monitoraggio si deve cliccare sulla prima icona a sinistra sulla barra degli strumenti. Compare una finestra da cui scegliere la scheda di rete attraverso la pressione del pulsante Start. È possibile attivare una singola scheda di rete attiva nel sistema oppure tutte le schede di comunicazione presenti. Sono contemplate le schede Ethernet ma anche interfacce IEEE 802.11, ATM, Token Ring, FDDI, ecc.



2 Il traffico che fluisce attraverso la scheda di rete selezionata viene catturato, decodificato e visualizzato sul pannello del software in maniera testuale. La finestra principale scorre in automatico per mostrare il traffico più recente. È possibile fermare lo scroll automatico e concentrarsi su porzioni specifiche di traffico. Nel caso sia necessario è possibile anche salvare il traffico su un file binario per eseguire decodifiche in futuro o per archiviare campioni di traffico.





3 È possibile evidenziare una singola riga di traffico dalla finestra principale per osservare la sua decodifica più in basso. Questa è strutturata in base alla gerarchia ISO OSI (di cui abbiamo già parlato) e per ogni livello è possibile osservare i valori di tutti i flag di protocollo. Più in basso c'è anche il dump esadecimale del pacchetto.

4 La potenza di Wireshark sta nella grande quantità di strumenti di analisi e di statistica sul traffico. Per esempio è interessante notare quante conversazioni sono in corso e quanto traffico è stato generato nell'ambito di queste conversazioni. Questo genere di analisi, per esempio, si può svolgere a livello di trame Ethernet, sui pacchetti IP o sui protocolli TCP e UDP.

ALLAH AKBAR:
Ubuntu Muslim Edition
Il pinguino al servizio di Maometto

La libertà e gratuità di GNU/Linux e del suo ecosistema software sono alla base delle innumerevoli versioni del sistema operativo che ha per simbolo un pinguino. Alcune si rivolgono a chi si occupa di sicurezza, altre ai creativi multimediali e altre ancora fanno concorrenza al salotto digitale di Microsoft. Ci sono poi le versioni localizzate per particolari paesi, lingue e culture ed è in questa categoria che rientra UbuntuME. Non si tratta di un rimando al famigerato WindowsME: le due iniziali finali stanno per "Muslim Edition" e la distribuzione è una personalizzazione di Ubuntu Linux rivolta a studiosi e devoti di religione musulmana



:: UbuntuME

La differenza principale rispetto alla versione standard è che UbuntuME (http://www.ubuntume.com/) include software e contenuti islamici per il momento della preghiera e lo studio del Corano, ma non solo.

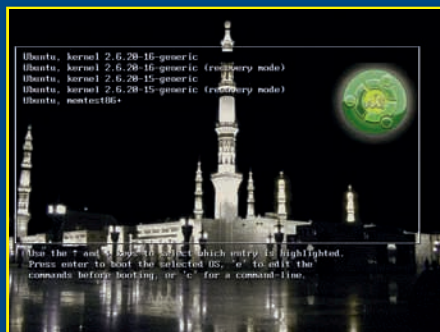
L'ultima release disponibile è la 8.04.1, che consigliamo di reperire attraverso DistroWatch (http://distrowatch.com/table.php?distribution=ubuntume), più aggiornato del sito ufficiale. Totalmente gratuita, UbuntuME è ora scaricabile come immagine DVD da poco meno di 4GB (http://distrowatch.com/?newsid=05004) ma in precedenza era distribuita sotto forma di due CD.

È ovviamente incluso l'ambiente grafico Gnome e tutti i software di produttività personale, da ufficio e per la navigazione e comunicazione come OpenOffice, Firefox, Thunderbird, Evolution, Gimp, Scribus, Skype, Adobe Reader ma il punto di forza di UbuntuME è altrove.



:: Gli strumenti

La cura messa in UbuntuME è notevole e appare sin dall'inizio sia sul versante grafico (con sfondi, temi, ecc.) che su quello funzionale con l'installazione di pacchetti di localizzazione (per Gnome, la Console e Mozilla Firefox) nonché font arabi e curate personalizzazioni (persino di grub). Ma l'aspetto più interessante è l'inclusione (e settaggio) di strumenti e contenuti specifici per l'utenza musulmana ed per le sue esigenze religiose.



Il principale è Zekr (http://zekr.org) in versione 0.7.0: si tratta di un software multipiattaforma in Java per lo studio del Corano. Permette di consultare o ricercare il testo sacro mostrando anche la traduzione. Zekr, che è free e open ed evidenzia il motto "Non speculare sl profeta" è fornito sui supporti già configurato e incluso di numerosi file audio (circa 2GB, motivo della scelta del DVD) tratti dal sito www.versebyversequran.com per le recitazioni "offline".



Altro software è Minbar (http://djihed.com/MinBar) che calcola e avverte per tempo di pregare e un compito simile è svolto da un'estensione per il browser Firefox allegata, "Pray Times" (https://addons.mozilla.org/en-US/firefox/addon/4270). Sempre per questa esigenza c'è Monajat (https://launchpad.net/monajat), che fa apparire automaticamente un popup quando è il momento con il testo per



pregare. Troviamo poi Hjira, un calendario arabo, e Thwab, un'enciclopedia islamica elettronica portabile. Completa il set di strumenti l'inclusione di un sistema di "parental control" e cioè di filtri di contenuti osceni o "inappropriati" per la navigazione dei siti web.

È chiamato Webstrict (http://www.ubuntume.com/webstrict) ma altrove semplicemente WCC, Web Content Control, e come gli altri tool è già attivato di fabbrica nell'installazione di UbuntuME. Per i più curiosi in realtà si tratta di un front-end basato su Dansguardian (http://dansguardian.org/). e su Tinyproxy (http://tinyproxy.sourceforge.net/).

CONVERTITEVI!

Chi ha già installato Ubuntu e ha bisogno di quanto offerto dalla Muslim Edition può ottenerlo con una procedura avviata e selettiva. Sul sito ufficiale poco dopo la procedura di installazione è infatti descritto (http://www.ubuntume.com/it:installation#convert_a_standard_ubuntu_installation) anche come "convertire" una installazione standard di Ubuntu 8.04 o precedente a UbuntuME.
La procedura è composta dall'aggiunta del repository di UbuntuME nel file /etc/apt/sources.list e quindi nell'uso di aptitude (dopo averlo aggiornato) per aggiungere i pacchetti necessari.